Appendix 1

Information And Communications Technology (ICT)
Supply Chain Risk Management (SCRM) Task Force (TF)
Threat Evaluation Working Group: Threat Scenarios, CISA,
February 2020

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE

Threat Evaluation Working Group: Threat Scenarios

February 2020

This page is intentionally left blank.

EXECUTIVE SUMMARY

Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of Information and Communications Technology (ICT) (including the Internet of Things) product and service supply chains. C-SCRM covers the entire life cycle of ICT, and encompasses hardware, software, and information assurance, along with traditional supply chain management and supply chain security considerations.

In October 2018, the Cybersecurity and Infrastructure Security Agency (CISA) launched the ICT Supply Chain Risk Management Task Force, a public-private partnership to provide advice and recommendations to CISA and its stakeholders on means for assessing and managing risks associated with the ICT supply chain. Working Group 2 (WG2), Threat Evaluation, was established for the purpose of the identification of processes and criteria for threat-based evaluation of ICT suppliers, products, and services.

WG2 focused on threat evaluation as opposed to the more comprehensive task of risk assessment which considers threats as well as an organization's tolerance for risk, the criticality of the specific asset or business/mission purpose, and the impact of exploitation of specific vulnerabilities that might be exploited by an external threat. The WG Co-chairs leveraged the National Institute of Standards and Technology (NIST) Risk Management Practices described in NIST SP 800-161 to help guide the analysis of the threats and threat sources identified in this work effort.

The general steps depicted in the figure below, and described in the following paragraphs, were used in the development and analysis of SCRM threats related to suppliers:

The WG membership were asked to identify a representative sample of the top SCRM threats specifically focused on suppliers in accordance with our initial proposed scoping. Once the threats were identified, the WG proceeded to compile additional information fields identified in NIST SP 800-161 as elements to capture and refine with the WG members.

Each of the identified threats was then reviewed by the WG to develop a proposed set of common groupings and category assignments to organize the identified threats. Based on the presentation and analysis of the threats submitted by the WG members, the threats were aggregated into a smaller, more manageable set of common "threat grouping" to aid in the evaluation process. The objective of the aggregation was to reduce the threat data and identify common elements for further evaluation using a scenario development process.

This grouping and descriptive titles were shared with the WG membership for review and comment. While consensus was not unanimous, it was determined that for the purposes of the evaluation scope, the list of nine categories represented a reasonable model for aggregation for this interim work product. These threat groupings served to guide the development of scenarios intended to provide insights into the processes and criteria for conducting supplier threat assessment.

For each category, the WG assembled teams to develop a narrative/scenario in a report format that included background information on the threat itself, the importance of this threat, and potential impact on the supply

chain. Multiple scenarios were developed for each category if deemed appropriate by the writing teams. A common format was developed to ensure that each threat scenario presented a comprehensive view of the specific threat aligned to the requirements of the information fields identified from NIST SP 800-161.

The process and resulting narratives not only serve as a baseline evaluation of specific SCRM threats, but further can be used as exemplary guidance on the application of the NIST Risk Management Framework. This process can be extended for evaluation of products and services, as well as replicated for other critical infrastructure providers. It also established a solid threat source evaluation that can be extended for specific products or services to drive the evaluation of SCRM risk.

Contents

Figures

Tables

1.0 THREAT EVALUATION WORKING GROUP TEAM MEMBERS

Leadership team for WG:

TABLE 1—LEADERSHIP AND ADMINISTRATIVE SUPPORT FOR WORKING GROUP 2

Co-Chair:	Drew Morin	T-Mobile
	Tommy Gardner	HP
	Angela Smith	GSA
Project Manager:	Julian Humble	DHS (SED)
Admin Support:	Josh Hyde	Contract Support (SED)
	Jaime Fleece	Contract Support (SED)

WG consists of the members listed below:

TABLE 2—COMMUNICATIONS SECTOR WORKING GROUP MEMBERS

Name	Company
Rich Mosely	AT&T
Jeff Huegel	AT&T
Jon Gannon	AT&T
Chris Boyer	AT&T
Kathryn Condello	CenturyLink
John Hayat	CenturyLink
Fernando Boza	CenturyLink
David Mazzocchi	CenturyLink
Dwight Steiner	CenturyLink
Melissa Brocato-Bryant	CenturyLink
Stephen Boggs	Cox
Rob Cantu	CTIA
Mike Kelley	E.W. Scripps Company
Eric Neel	Hubbard Broadcasting
Michael Iwanoff	Iconectiv
Larry Walke	National Association of Broadcasters
Kelly Williams	National Association of Broadcasters
Matt Tooley	NCTA
Jesse Ward	NTCA
Shamlan Siddiqi	NTT
Chad Kliewer	Pioneer
Mike Funk	Quincy Media
Diana Keplinger	Sprint
Greg Holzapfel	Sprint
Savannah Schaefer	TIA

Name	Company
Tanya Kumar	T-Mobile
Jessica Thompson	U.S. Telecom
Robert Mayer	U.S. Telecom
Michael Saperstein	U.S. Telecom
Frank Frontiera	Verizon
Chris Oatway	Verizon

TABLE 3—INFORMATION TECHNOLOGY SECTOR WORKING GROUP MEMBERS

Name	Company
Tom Topping	FireEye
Robert Wharton	HPE
C.J. Coppersmith	HPE
Ion Green	HPE
Mark Kelly	Dell
Trey Hodgkins	Hodgkins Consulting, LLC
John S. Miller	ITIC
Christopher "Travis" Miller	Interos
David Flowers	Interos
Randi Parker	CompTIA
Alvin Chan	HP
Melissa Bouilly	Dell
Tommy Ross	BSA
Jon Amis	Dell
Audrey Plonk	Intel
Ari Schwartz	Coalition for Cybersecurity Policy & Law
Geoff Kahn	Accenture
Marty Loy	Cisco
Jamie Brown	Tenable
Brad Minnis	Juniper - ITIC
Nick Boswell	CDW-G
Charlotte Lewis	CDW-G
Corey Cunningham	Rehancement Group
Peter McClelland	Threat Sketch
Tina Gregg	Microsoft
Jacob Crisp	Microsoft
Jason Boswell	Ericsson
Steve Lipner	SAFECode
Eric Nelson	Rehancement Group

TABLE 4—U.S. GOVERNMENT WORKING GROUP MEMBERS

Name	Company
Debra Jordan	FCC
Kurian Jacob	FCC
Dennis Martin	DHS
Ronald Clift	DHS
Beatrix Boyens	DHS
Michael Van de Woude	GSA
Jeremy P. McCrary	EOP/OMB
Jeffery Goldthorp	FCC
Rui Li	NRC
Patrick J. Kelly	OCC/Treasury
John Bowler	OCC/Treasury
Bradford "Brad" Bleier	FBI
Celia Paulsen (Prime)/Jon Boyens (Backup)	NIST
Michael Van de Woude	GSA
Gwen Hess	DHS
Scott Morrison	DOJ
Keith Nakasone (Prime)/Kelley Artz (Backup)	GSA
Stacy Bostjanick	DOD
Cherylene G. Caddy	NSA
Anita J. Patankar-Stoll	NSC
Evan Broderick	NTIA
Megan Doscher	NTIA
Scott Friedman	DHS
Evelyn Remaley	NTIA
Ganiu "Tosin" Adegun	NASA
Michael "Mike" Bridges	NASA
Kanitra Tyler	NASA

2.0 BACKGROUND

In October 2018, CISA launched the Information and Communications Technology Supply Chain Risk Management (ICT SCRM) Task Force, a public-private partnership to provide advice and recommendations to the CISA and its stakeholders on means for assessing and managing risks associated with the ICT supply chain.

The ICT SCRM Task Force provides a mechanism for representatives of industry and government, designed to share information, explore challenges, and develop recommendations to manage ICT supply chain risks. The Task Force is led by representatives of DHS and the Communications and Information Technology sectors. Task Force membership and participation represents the public-private, cross-sector nature of the Task Force, with members drawn from both sectors and from across the government.

The Task Force summarized the results of its first year of work in the ICT SCRM Task Force Interim Report, which was released in September 2019 and can be found HERE (https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf). This Interim Report includes a description of the Task Force's progress and an initial set of recommendations, derived from the individual reports of the Task Force's four WGs. The Interim Report and the reports of the subordinate WGs memorialize the work of these collaborative bodies, including consensus recommendations provided through the Critical Infrastructure Partnerships Advisory Council process to the federal agency participants. The activity of federal employees on the task force, including participation in discussions and votes, is intended to inform the Task Force's work through the individual experience of the participating members as subject matter experts and does not necessarily represent the official position of, or adoption of any recommendation by, the U.S. government or any represented Federal department or agency.

The Task Force evaluated multiple potential work streams and reached consensus on the establishment of four Task Force WGs and an Inventory WG. WG, Threat Evaluation, was established for the purpose of the **identification of processes and criteria for threat-based evaluation of ICT suppliers, products, and services**. This proposed work stream is intended to provide ICT buyers and users with assistance and guidance for evaluating supply chain threats. Bringing uniformity and consistency to this process will benefit government and industry alike.

2.1 Relationship between Threat, Vulnerability, and Risk

A thing (threat source) interacts with a weakness (vulnerability) which results in something bad happening (threat event). The way the source interacted with the weakness is a *threat vector*. If the threat source was a human and the event intentional, it is an *attack*.

A vulnerability is a shortcoming or hole in the *security* of an asset. Risk represents the potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. Risk is the intersection of assets, threats, and vulnerabilities.

2.2 Relevant Definitions

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (FIPS 200)

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. (FIPS 200)

Threat event: An event or situation that has the potential for causing undesirable consequences or impact. (NIST SP 800-30)

Threat source / agent: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. (FIPS 200)

Attack: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality. (NIST SP 800-82 & CNSSI 4009)

3.0 OBJECTIVE, SCOPE, AND METHODOLOGY

Working Group 2 is focused on Threat Evaluation as opposed to risk assessment since risk is specifically associated with an asset (product, service, supplier in the case of the charter for this ICT C-SCRM Task Force).

The WG Co-chairs leveraged the NIST Risk Management Practices described in NIST SP 800-161 to help guide the analysis of the threats and threat sources identified in this work effort.

3.1 Objective

ICT Task Force WG, Threat Evaluation, was chartered with the identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services. The objectives of this Threat Evaluation were defined as:

- Produce a set of processes and criteria for conducting supplier, product, and service threat assessments.
- The processes and criteria will initially be focused only on global ICT supplier selection, pedigree, and provenance. It will also address product assurance (hardware, software, firmware, etc.), data security, and supply chain risks.
- Finally, the process and criteria will establish a framework for a threat-based assessment of cyber supply chain risks that can be extended in future work products to address other critical infrastructure sectors.

3.2 Scope

The ICT C-SCRM Task Force agreed early on to leverage the NIST definition for C-SCRM and to scope according to the Federal Acquisition Supply Chain Security Act.

NIST definition: Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of ICT product and service supply chains. C-SCRM covers the entire life cycle of ICT:

- Encompasses hardware, software, and information assurance, along with traditional supply chain management and supply chain security practices.[1]

Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Subchap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018)

Covered articles means:

- Information technology, including cloud computing services of all types (41 USC 4713(k)(2)(A));
- Telecommunications equipment or telecommunications service (41 USC 4713(k)(2)(B));
- The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (41 USC 4713(k)(2)(C));
- All Internet of Things/Operational Technology (IoT/OT) – (hardware, systems, devices, software, or services that include embedded or incidental information technology). (41 USC 4713(k)(2)(D)).

[1] See, NIST definition of C-SCRM, available at: https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management. For purposes of the ICT SCRM Task Force, the term "ICT" includes operational technology and "Internet of Things" devices and services.

3.3 Methodology

The WG initially conducted a survey of threat information from the diverse WG membership. The only constraint on the identification of threats was to focus on supplier threats in accordance with our initial proposed scoping. The methods developed and applied in our initial supplier threat evaluation process will be repeatable in future iterations as the WG proceeds to expand our scope to include products and services.

Once the threats were identified, the WG proceeded to complete the additional information captured in the fields highlighted in green from the NIST SP 800-161 spreadsheet in table 5 below as elements to capture and refine with the WG members. Information was captured in the current WG2 Supply Chain Threats by adding a few additional columns. This information was then used to inform the threat analysis process for supplier evaluation.

TABLE 5—TABLE DERIVED FROM NIST SP 800-161

Threat Scenario	**Threat Source**	*Threat "actor" or category of threats*
	Vulnerability	*Threat list Working group has generated*
	Threat Event Description	*Description of the method(s) of exploiting the vulnerability*
	Outcome	*Description of potential impacts to Supply Chain or consequences of exploiting the vulnerability*
Organizational units / processes affected		*This should reflect how/where in the supply chain the impact occurs*
Risk	**Impact**	
	Likelihood	
	Risk Score (Impact x Likelihood)	
	Acceptable Level of Risk	
Mitigation	**Potential Mitigating Strategies / SCRM Controls**	*Identify supplier evaluation criteria that would reduce or mitigate the impact of the threat*
	Estimated Cost of Mitigating Strategies	
	Change in Likelihood	
	Change in Impact	
	Selected Strategies	
	Estimated Residual Risk	

The remaining fields not completed by this WG represent the asset specific data that is captured to assess risk; something that will vary considerably depending on the specific supplier/product/service. This will result in a work product that will be consistent with NIST guidance concerning threat and flexible to be used by industry and public sector for a variety of purposes.

The WG executed using an iterative process with interim deliverables shareable between the other Task Force WGs to inform their efforts. For example, the threats identified by WG2 were shared with and used to inform the Information Sharing WG on threat focus areas for information gathering and sharing. Similarly, the threats identified were leveraged to aid in assessing the inventory of standards and best practices that may be applicable to the evolving C-SCRM threat environment.

3.3.1 FOCUS ON SUPPLIER THREATS — DATA GATHERING PROCESS

This section describes the process used to generate the threats to SCRM suppliers and the sharing of those threats as inputs to the evaluation to follow. It should be noted that these threats are not considered comprehensive, but rather are representative, such that the evaluation WG could proceed through the exercise of threat evaluation put forward by the NIST Risk Management Framework.

The WG members considered C-SCRM Threats from a variety of sources including Industry Subject Matter Experts (SME), Department of Defense (DoD), Intelligence Community (IC), Department of Homeland Security (DHS), and others to inform the development of risk-based criteria. The first data call conducted was a request from WG membership to provide supply chain threats that they recognize from their own experience or from their organization's perspective.[2] The requested format of the data call was a bulleted list describing each threat. Our purpose was to initially cast a wide net to capture a broad sample of threat inputs for analysis.

Each threat submitted was presented by the WG member that sourced the information to the broader membership. The discussion enabled the WG to process additional details on each threat with the stated purpose of gaining a shared understanding of the specific threats identified. This process was repeated, and notes were captured for each of the identified threats. This set of information was compiled into a single data repository that was used in the Data Analysis phase of the process described below.

3.3.2 DATA ANALYSIS

The WG proceeded to review and categorize the collected data to develop useful insights into the current state of supplier threats in both public and private sectors. The threats identified by the WG members were then consolidated and grouped to provide a manageable and shareable set of threat groupings for further the development of specific scenarios. These threat groupings served to guide the development of scenarios intended to provide insights into the processes and criteria for conducting supplier threat assessment.

As part of our analysis, the WG membership considered existing business due diligence indicators, such as those listed in General Services Administration's (GSA) Request for Information (RFI), Office of the Comptroller of the Currency (OCC) Third Party Risk Management guidance, and industry best practices identified as part of the inventory work product. Figure 1 below depicts the flow used by the WG to conduct the data analysis.

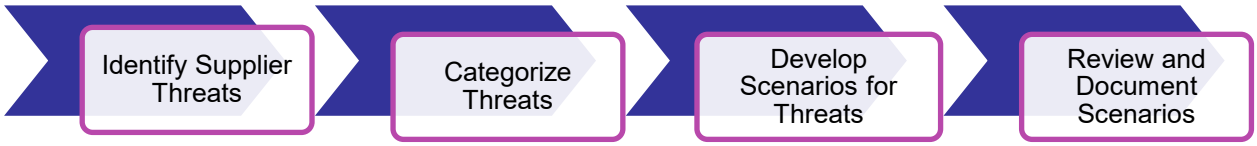


FIGURE 1—DATA ANALYSIS WORKFLOW

[2] The working group data call requested each member to provide between five and ten supplier threats. The result was an initial set of over 250 specific threats.

3.3.3 THREAT SCENARIO DEVELOPMENT

Once the WG has established supply chain threat categories, the WG assembled teams for each category. Each team then provided a narrative/scenario developed in a report format that includes **background information on the threat itself, the importance of this threat, and potential impact on the supply chain**. Multiple scenarios were developed for each category if deemed necessary by the writing teams. Each scenario also includes details surrounding the:

- **What** (Description of the threat category. Text could include example threats associated with the category),
- **Who** (Who is likely to be the source of the threat [e.g., nation state, organized crime] and who the likely target of the threat is),
- **When – If applicable** (Is the timing of the attack? Is it Denial of Service or zero day? Is it persistent or a one-time event? Etc.),
- **Why** (Objective of threat actors, intellectual property theft, network disruption…), and
- **Where** (Where in the Supply chain the specific threat activity is occurring).

A common format was developed to ensure that each threat scenario presented a comprehensive view of the specific threat aligned to the requirements of the information fields identified from NIST SP 800-161 as described in Section 2.0 above.

4.0 FINDINGS

4.1 Supplier Threat List

This section describes the supplier threat information gathered and the specific information for each threat that was presented for evaluation by the WG membership.

4.1.1 TAXONOMY OF THREAT LIST

The initial data call from the WG members was for the identification of supplier threats. The scope of the threats was intentionally left broad to not restrict the identification process. A limited set of information was provided for each threat by the WG member that sourced the information.

- Threat description: Short text description of the specific supplier threat
- Threat category (provided by source): Identification of the category that the WG member assigned to the identified threat
- Threat source: Identification of the source or sources that might exploit the vulnerability identified by the threat

4.1.2 THREAT LIST

The threats identified were presented to the entire WG to enable a common understanding of the information provided concerning each specific threat. The list was then consolidated based on common threat categories and reviewed with the WG membership to gain consensus.

4.2 Threat Data Analysis

4.2.1 CATEGORIZATION OF THREATS

Once the threat list was populated, the co-chairs reviewed the categories assigned to each of the threats to aggregate specific threats into a smaller, more manageable set of common threat groups. The objective of the

aggregation was to reduce the threat data and identify common elements for further evaluation using a scenario development process.

In order to aggregate the data, common threat categories were first identified. The next step of the analysis was to group the threats that shared common and related threat categories. Each of the identified threats was then reviewed by the WG to ensure that the common groupings and category assignments accurately reflected the threat. A few of the threats initially identified were dropped from the list as they did not actually represent threats (for example, some were impacts or use case specific risks).

Once the threat category review was completed, the co-chairs proposed a set of threat groups to represent the set of common categories of threats identified. This grouping and descriptive titles were shared with the WG membership for review and comment. While consensus was not unanimous, it was determined that for the purposes of the evaluation scope, the list of nine categories represented a reasonable model for aggregation.

4.2.2 DESCRIPTION OF THREAT GROUPS

The evaluation of the threats submitted by the broad spectrum of WG members was consolidated into logical threat groups to aid in the evaluation process. The description of each of these threat groupings is provided in the following sections.

4.2.2.1 Counterfeit Parts

Insertion of counterfeits in the supply chain can have severe consequences in systems and services provided to downstream customers. These threats are associated with the replacement or substitution of trusted or qualified supplier components, products, or services with those from potentially untrusted sources.

4.2.2.2 Cybersecurity

This threat category represents those that result from the set of vulnerabilities associated with external attacks on suppliers' operations and capabilities. These threats are the result of an external actor exploiting a vulnerability or planting malware attack such as zero day or malware with an objective of compromising the confidentiality, integrity, or availability of the supplier information, products, or services.

4.2.2.3 Internal Security Operations and Controls

This category of threats is closely related to cybersecurity identified above. The primary differentiator is that these threats are a result of challenges in internal supplier processes that enable the exploitation of weaknesses in basic cyber hygiene (e.g., software patching), user awareness (e.g., spear phishing), mishandling of sensitive information, or internal cybersecurity process failures from the lack of a cybersecurity program based on best practices such as the NIST Cybersecurity Framework.

4.2.2.4 System Development Life Cycle (SDLC) Processes and Tools

This threat category represents those threats that impact the suppliers' ability to develop products or services that protect the confidentiality, integrity, and availability of products and services developed by the supplier.

An example of this group of threats include failures in the development process to detect introduction of malware or unvetted code into software products through use of vulnerable open source libraries.

4.2.2.5 Insider Threats

This category of threats focuses on the vulnerability of the supplier to attack from trusted staff and partners that are embedded internal to the supplier operations. Most of the threats identified in this grouping are associated with intentional tampering or interference.

4.2.2.6 Economic Risks

Economic risks stem from threats to the financial viability of suppliers and the potential impact to the supply chain resulting from the failure of a key supplier as a result. Other threats to the supply chain that result in economic risks include, but are not limited to, vulnerabilities to cost volatility, reliance on single source suppliers, cost to swap out suspect vendors, and resource constraints as a result of company size.

4.2.2.7 Inherited Risk (Extended Supplier Chain)

This category of threats is a result of current supply chains that extend broadly across industries and geographies. These threats typically are associated with the challenge of extending controls and best practices through the entire supply chain due to its global nature. It also includes the vulnerabilities that can result from integration of components, products, or services from lower tier supplier where a prior determination of acceptable risk may not flow all the way through the development process to the end user supplier.

4.2.2.8 Legal Risks

This category of threats emanates from supplier vulnerabilities specific to legal jurisdiction. Some examples include weak anti-corruption laws, lack of regulatory oversight, weak intellectual property considerations. This also includes the threats that result from country specific laws, policies, and practices intended to undermine competition and free market protections such as the requirement to transfer technology and intellectual property to domestic providers in a foreign country.

4.2.2.9 External End-to-End Supply Chain Risks (Natural Disasters, Geo-Political Issues)

This category of threats is associated with broad based environmental, geopolitical, regulatory compliance, workforce and other vulnerabilities to the confidentiality, integrity or availability of supplier information, products or services.

4.2.3 THREAT LIST INCLUDING THREAT GROUPS

The threat list compiled based on the data analysis presented is included as Appendix B to this document.

4.3 Threat Scenarios

4.3.1 SCENARIOS

The Threat Evaluation WG – Supplier Threat Scenarios developed for the ICT SCRM Task Force is included as Appendix C to this document.

5.0 CONCLUSIONS

The WG kicked off this evaluation with a blank sheet and focused on leveraging the diversity of our membership to provide a broad base of threats for analysis and evaluation.

This interim report and threat evaluation is limited to supplier threats only. The WG membership recognize that some of these threats are also applicable to products and services.

The methods developed and applied in our initial supplier threat evaluation process will be repeatable in future iterations as the WG proceeds to expand our scope to include products and services.

The WG struggled with the specific threat groupings used, including proposal for further aggregation of the threat groupings into common sets to provide further clarification of the definition of each threat grouping. There were also some concerns that the threats identified may have also included risks. Due to time

constraints, the co-chairs captured this information but decided to defer this to potential follow on work on products and services. This assumes that the task force supports the WG guidance to continue this work effort in the next iteration of WG outputs.

The WG recommends that the task force continue the charter for this effort with a focus on addressing products and services, review of categorization of threats, and possibly to provide risk assessments of some specific threats, prioritized by membership, as examples of how to leverage this threat assessment as an information feed into a company specific risk management program.

APPENDIX A: ACRONYM LIST

BGP	Border Gateway Protocol
BIA	Business Impact Analysis
CAD	Computer-Assisted Design
CCTV	Close-Circuit Televisions
CERT	Computer Emergency Readiness Team
CFIUS	Committee on Foreign Investment in the United States
CIS	Center for Internet Security
CSRIC	Communication, Security, Reliability, and Interoperability Council
C-SCRM	Cyber Supply Chain Risk Management
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
DOJ	Department of Justice
EAS	Emergency Alert System
FAR	Federal Acquisition Regulation
FCC	Federal Communications Commission

FIPS	Federal Information Processing Standards
GSA	General Services Administration
HPE	Hewlett-Packard Enterprises
ICT	Information and Communications Technology
ID	Identification
IP	Internet Protocol
IP*	Intellectual Property
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITAM	Information Technology Asset Management
ITIC	Information Technology Industry Council
ITP	Insider Threat Program
MAC	Media Access Control
MANRS	Mutually Agreed Norms for Routing Security
NASA	National Aeronautics and Space Administration
NDA	Non-Disclosure Agreement
NIST-SP	National Institute of Standards and Technology (NIST) Special Publication

NTIA	National Telecommunications and Information Administration
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OS	Operating System
OT	Operational Technology
PAM	Privileged Access Management
PC	Personal Computer
PCB	Printed Circuit Board
PWB	Printed Wiring Board
SAM	Software Asset Management
SC	Semiconductor
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SED	Stakeholder Engagement Division
SMB	Small and Medium-sized Business
SNMP	Simple Network Management Protocol
SPVM	Sourcing, Procurement and Vendor Management
SQL	Standardized Query Language

SSH	Secure Shell
TAA	Trade Agreements Act
TIA	Telecommunications Industry Association
U.S.	United States
USB	Universal Serial Bus
VPN	Virtual Private Network
WG	Working Group

APPENDIX B: THREAT LIST

Note: The WG membership were asked to identify a representative sample of the top SCRM threats specifically focused on suppliers in accordance with our initial proposed scoping. Based on presentation and analysis of the threats submitted by the WG members, the items were aggregated into a smaller, more manageable set of common threat groupings to aid in the evaluation process. The objective of the aggregation was to identify common elements for further evaluation using a scenario development process. The threats identified represent the output produced by this methodology, and do not represent an official or consensus documentation of supply chain threats. The threat list is intended to document the WG's work and provide input for future policy discussions.

Threats	Threat Categories or Event	Threat Source or Actor
Counterfeit Parts		
Counterfeit product or component with malicious intent to cause unwanted function	Adversarial: Craft or create attack tools	Nation state; organization; individual (Outsider/Insider)
Component elements included in product, software, or service		
Virtualization and encapsulation hiding access		
Sales of modified or counterfeit products to legitimate distributors		
A malicious supplier employee inserts hostile content at the product or component manufacturing or distribution stage so as to affect supplier products or components delivered to a subset (potentially a targeted subset) of downstream customers. (Tampering or counterfeiting)		
Insert tampered critical components into organizational systems	Adversarial: Deliver, insert, or install malicious capabilities	

Insert counterfeit or tampered hardware into the supply chain		Nation state; Organization; Individual (Outsider/Insider)
Counterfeit product or component without malicious intent to cause unwanted function	Accidental: User; privileged user	Individual (Insider)
Create counterfeit or spoof website	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Craft counterfeit certificates	Adversarial: Craft or create attack tools	Nation state; Organization
Embedded HW/SW threats from non-OEM source(s)	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Cybersecurity		
Data breaches and unauthorized access to sensitive data (at rest and in transit)	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider/Insider)
Loss of critical information from vendor		
Obtain unauthorized access		
Data - Impacts to confidentiality, Integrity or availability		
Malware, unauthorized access, theft		
Cause unauthorized disclosure or unavailability by spilling sensitive information		
Spill sensitive information	Accidental: User; privileged user	Individual (Insider)

Login Attacks (Brute force, Dictionary attacks, Password spraying)	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider)
Credential Compromise		
Supplier solution architecture allows for manipulation and extraction of data and services (Not due to a system vulnerability)	Accidental: User, privileged user	Nation state; Organization; Individual (Outsider/Insider)
Phishing, spear phishing, or whaling	Adversarial: Craft or create attack tools	Nation state; Organization;
Malware, unauthorized access, theft		
Deliver known malware to internal organizational information systems (e.g., virus via email)	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider)
Compromise of integrity of product through intrusion	Adversarial: Exploit and compromise	Nation state; Organization; Individual (Outsider)
External cyber attacker threats		
Embedded malware or virus attacks in delivered products	Adversarial: Craft or Create Attack Tools	Nation state; Organization; Individual (Outsider/Insider)
Inappropriate modification of device, software, or service through network update		
Embedded HW/SW threats (from manufacturing)		

A malicious supplier employee inserts hostile content at the product or component manufacturing or distribution stage so as to affect supplier products or components delivered to a subset (potentially a targeted subset) of downstream customers. (Tampering or counterfeiting)		
Embedded Malware. Virus Attacks in hosted services websites	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Malware disguised as driver updates or system patches on compromise vendor web site		
Intrusion or compromise of customer through service		
Inappropriate modification of device, software, service through network update		
Product vulnerabilities (intended) in hardware and software	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Product vulnerabilities (unintended) in hardware and software	Accidental: User, privileged user	Individual (Insider)
Resource depletion		
Pervasive disk error		
Advanced Persistent Threats	Adversarial: Maintain a presence	Nation state; Organization
DNS attack	Adversarial: Conduct an attack	Nation state; Organization
DoS/DDoS	Adversarial: Conduct an attack	

Threat actor impacts app store availability impacting end user ability to do job		Nation state; Organization; Individual (Outsider)
Threat actor hacks cloud environment or telco making service unavailable		
Threat actor breaks ability of information provider to deliver information		
Man in the middle attack	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider)
Obtain information by externally located interception of wireless network traffic		
Incorrect BGP routing at a level above your network		
Replay attack	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider)
Spoofing	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider)
URL injection	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider)
Intentional specific software security threats or vulnerabilities exploitation (long list of specific types not included for brevity)	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Threat actor compromises or hacks it software		
Unintentional specific software security threats or vulnerabilities exploitation (long list of specific types not included for brevity)	Accidental: User, privileged user	Individual (Insider)

System misconfiguration	Accidental: User, privileged user	Nation state; Organization; Individual (Outsider/Insider)
Zero-Day exploits	Adversarial: Craft or create attack tools	Nation state; Organization
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware	Adversarial: Conduct an attack (i.e., direct or coordinate attack tools or activities)	Nation state; Organization
Perform malware- directed internal reconnaissance	Adversarial: Perform reconnaissance and gather information	Nation state; Organization
Craft attacks specifically based on deployed information technology environment	Adversarial: Craft or create attack tools	Nation state; Organization
Deliver modified malware to internal organizational information systems	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Deliver targeted malware for control of internal systems and exfiltration of data	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Deliver malware by providing removable media	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization
Exploit split tunneling	Adversarial: Exploit and compromise	Nation state; Organization
Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo	Adversarial: Exploit and Compromise	Nation state; Organization; Individual (Outsider/Insider)

Violate isolation in multi-tenant environment	Adversarial: Exploit and Compromise	Nation state; Organization
Compromise information systems or devices used externally and reintroduced into the enterprise	Adversarial: Exploit and Compromise	Nation state; Organization
Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome	Adversarial: Maintain a presence or set of capabilities	Nation state; Organization
Coordinate cyber-attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors	Adversarial: Maintain a presence or set of capabilities	Nation state; Organization
Purchasing of equipment with known critical security vulnerabilities (example: nearly all Android based cellphones) and little expectation of patching by vendor	Accidental: User, privileged user	Individual: Insider
Compromise of integrity of virtualization	Adversarial: Exploit and compromise	Nation state; Organization; Individual (Outsider/Insider)
Access through service contract	Adversarial: Maintain a presence or set of capabilities	Nation state; Organization
Quantum computing threat to commercial cryptography	Adversarial: Exploit and compromise	Nation state
Cryptojacking	Adversarial: Exploit and compromise	Nation state; Organization
Ransomware	Adversarial: exploit and compromise	Nation state; Organization
Conduct physical attacks on infrastructures supporting organizational facilities	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider/Insider)
Physical compromise of specific device		

Physical access through presence of device	Adversarial: Exploit and compromise	Nation state; Organization; Individual (Outsider/Insider)
Physical network control or access		
Physical control of infrastructure		
Threat actor activity overwhelms organizations ability to deal with attacks, IT supply chain-services unable to surge to meet need	Adversarial: Conduct an attack	Nation state; Organization
Internal Security Operations and Controls		
Lack of knowledge (suppliers or subcontractors, especially SMBs, not knowing what their vulnerabilities are)	Accidental: Deliver, insert, install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Product vulnerabilities (advertent or inadvertent) in hardware and software	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Vulnerability Exploitation		
Supplier Has Weak Controls To Detect Or Prevent Social Engineering	Accidental: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider)
Data And Media Disposal Is Not Secure-Allowing Disclosure Of Sensitive Data	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider)
Obtain information by opportunistically stealing or scavenging information systems/components.		
Exploit insecure or incomplete data deletion in multi-tenant environment.	Adversarial: Exploit and Compromise	Nation state; Organization; Individual (Outsider)
Data breaches post disconnect		

Poor Employee/Contractor/Vendor Access Controls	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider/Insider)
Supplier System Does Not Have Controls To Validate And Authorize Escalation Of Privileges		
Staff using vulnerable unpatched personal computer systems from home to contact agency resources	Accidental: Individual	Individual (Outsider/Insider)
Large enterprise (~$10 billion / year) that supplies key components for mission projects continues to experience cyberattack and illicit technology transfer events	Adversarial: Exploit and Compromise	Nation state; Organization; Individual (Outsider)
ICT Devices with default passwords	Accidental: Deliver, insert, or install malicious capabilities	Organization
(Removal of) Hardset accounts in devices and software		
Devices that do not auto-update firmware	Accidental: Deliver, insert, or install malicious capabilities	Organization
Mishandling of critical or sensitive information by authorized users	Accidental: Individual	Individual (Insider)
Incorrect privilege settings	Accidental: Individual	Individual (Insider)
The nuclear power section has a maturing cyber program or defense architecture and regulatory requirements, but sophisticated offensive groups with nation states capabilities are threats	Accidental: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider)
Compromise of SDLC Processes and Tools		
Malware coded, inserted, or deployed into critical ICT throughout the design,		

development, integration, deployment or maintenance phase of components	Adversarial: Craft or create attack tools	Nation state; Organization; Individual (Outsider/Insider)
Manipulation of development tools		
Manipulation of a development environment		
Manipulation of source code repositories (public or private)		
Manipulation of software update/distribution mechanisms		
Compromise design, manufacture, or distribution of information system components (including hardware, software, and firmware)	Adversarial Supply Chain Threat: Exploit and compromise	Nation state; Organization; Individual (Outsider/Insider)
Compromised/infected system images (multiple cases of removable media infected at the factory)	Adversarial: Exploit and Compromise	Nation state; Organization; Individual (Outsider/Insider)
Replacement of legitimate software with modified versions	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Insert untargeted malware into downloadable software or into commercial information technology products.		
Insert targeted malware into organizational information systems and information system components.	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Insert specialized malware into organizational information systems based on system configurations.	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Introduction of vulnerabilities into software products from open source	Accidental: Individual	Individual (Outsider/Insider)

Software integrity and does the product include open source code		
Foreign developed computer code or source code	Accidental: Individual or privileged user	Nation state; Organization; Individual (Outsider/Insider)
Foreign companies controlled or influenced by a foreign adversary	Adversarial: Maintain a presence or set of capabilities	Nation state
Insider Threat		
Lone wolf (disgruntled employee)	Adversarial: Conduct an attack	Individual: Insider
Insider threats	Adversarial: Deliver, insert, or install malicious capabilities.	Nation state; Organization; Individual (Outsider/Insider)
Threat actor recruits onsite IT services personnel with gambling debts to spy		
IT services supply chain sends spy onsite		
Insert subverted individuals into organizations		
Insert subverted individuals into privileged positions in organizations		
Internal: Personnel Threat		
Conduct internally based session hijacking	Adversarial: Conduct an attack	Individual: Privileged Insider
Tampering while on hand	Adversarial: Conduct an attack	Individual (Outsider/Insider)
Tampering while being deployed or installed	Adversarial: Conduct an attack	Individual (Outsider/Insider)

Tampering while being maintained	Adversarial: Conduct an attack	Individual (Outsider/Insider)
Tampering while being repaired	Adversarial: Conduct an attack	Individual (Outsider/Insider)
Economic		
Viability of financially weak suppliers	Economic: Financial stability	Nation state; Organization
Financial Stability	Economic: Financial stability	Nation state; Organization
Economic risk (i.e. a supplier or sub-contractor of a supplier will be economically devastated by a breach).	Economic: Financial stability	Nation state; Organization
Limited visibility into business and sustainability practices of suppliers beyond the first tier	Economic: Financial stability	Organization
Cost Volatility	Economic: Financial stability	Organization
No vendor support when a company transfers ownership or closes	Economic: Financial stability	Organization
Operational disruptions due to source being acquired by a far larger company with questionable security		
Very small, privately-held company "one-man show" with inadequate quality management with history of delivery delays and security concerns contracted to product components on the critical path of multiple mission projects	Economic: Financial stability	Organization
Young entrepreneurial business identified as a potential subcontractor for key mission components but has no discoverable facility for production, integration, test, nor quality management		

SMB often lack the ability to heavily influence vendors to correct issues	Economic: Production problems	Organization
Little control over what applications or devices customers use or connect via our services	Economic: Production problems	Organization; Individual (Outside)
If a vendor is compromised, some providers that use the same equipment or software across their entire system do not have the resources to continue operations or switch to another vendor	Economic: Production problems	Nation state; Organization; Individual (Outsider/Insider)
Threat Actor Determines How To Manipulate Decision By Delivering Too Much, Too Little, or Type of Information. It's Not Inaccurate, Yet It Somehow Changes Decisions	Economic: Production problems	Nation state; Organization; Individual (Outsider/Insider)
Industry Discovers Vulnerability In IT Product X Resulting In Freeze In Using That Product Until Fixed.	Economic: Production problems	Nation state; Organization; Individual (Outsider/Insider)
Small and many medium sized businesses do not have the resources or expertise to evaluate the security of all devices and software that are purchased by the company	Economic: Production problems	Organization
Most small and medium sized providers do not proactively monitor customer-based equipment for anomalous behaviors, and as such are unable to diagnose a security issue unless notified by other means	Economic: Production problems	Organization
Inherited Risk (Extended Supplier Chain)		
Inherited risk (extended supplier chain)	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Inherited risk generally		

Mid supply chain insertion of counterfeit parts		
Depth of the supply chain and who is supplying the supplier		
Domestic Companies		
Lack of enforced traceability		
Supplier incorporates hostile content in product or component		
Threat of upstream intrusions in supply chain and lack of traceability from component to finished product		
Supplier has malicious intent and incorporates hostile content in product or component. This scenario applies to hardware or software providers (including both proprietary and open source software)		
Trustworthy supplier inadvertently creates a product or component that is vulnerable to attack and delivers it to downstream customers. This scenario applies to hardware or software providers (including both proprietary and open source software).		
Tampering while in transit	Adversarial: Conduct an attack	Nation state; Organization; Individual (Outsider/Insider)
Shipment interdiction		
Vendor noncompliance	Adversarial: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Lack of Certification of component safety or quality at each appropriate level of the value chain of a product		

Integrity of integrated third-party components		
Lack of oversight or security standards for imported devices		
NRC does not have direct authority over third party suppliers.		
Lack of required disclosure of component manufacturer origin	Adversarial or Accidental: Deliver, insert, or install malicious capabilities	Nation state; Organization; Individual (Outsider/Insider)
Lack of disclosure of origin		
Create and operate false front organizations to inject malicious components into the supply chain	Adversarial: Craft or create attack tools	Nation state; Organization
IT information provider delivers intentionally bad or misleading data (e.g. DNS/BGP)	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider/Insider)
A malicious supplier employee inserts hostile content at the product or component design or software coding stage so as to affect a large number of supplier products or components. (Tampering)	Adversarial: Achieve results	Individual (Insider)
An upstream supplier to the trustworthy supplier serves as a vehicle (witting or unwitting) for introduction of hostile content into a hardware or software component that the trustworthy supplier in turn integrates into its product or component and delivers to downstream customers. (Tampering or counterfeiting)	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider/Insider)
An external threat actor penetrates the trustworthy supplier's design or manufacturing systems and inserts hostile content into a product or component that the trustworthy supplier	Adversarial: Achieve results	Nation state; Organization; Individual (Outsider)

delivers to downstream customers (Tampering)		
Legal risks		
Legal: IP or Licensing violation	Legal: IP or Licensing violation	Nation state; Organization; Individual (Outsider/Insider)
Suppliers operating in countries with weak Intellectual Property (IP) protection laws		
Liability for purchaser	Legal: Lawsuits	Nation state; Organization
Supplier fear liability impact could devastate participants in supply chain, particularly SMBs	Legal: Lawsuits	Nation state; Organization; Individual (Outsider/Insider)
Privacy regulations	External: Government compliance and political uncertainty	Nation state; Organization
Legislation and compliance	External: Government compliance and political uncertainty	Nation state; Organization
Known to engage in financial crimes (e.g. fraud, bribery, money laundering, etc.)	External: Legal noncompliance or ethical practices	Organization
Known to have violated U.S. sanctions		
External, End-to-End Supply Chain Risks		
Natural disaster causing supply chain disruptions	External: Natural disasters	Environmental: Natural
Natural disaster		
Natural disruptions		

Geo-Political uncertainty	External: Government compliance and political uncertainty	Nation state; Organization
Man Made Disruptions: sabotage, terrorism, crime, war	External: Government compliance and political uncertainty	Nation state; Organization
Labor issues	External: Government compliance and political uncertainty	Nation state; Organization
Supply chain disruptions and price spikes due to protectionism in global trade	External: Government compliance and political uncertainty	Nation state
Lack of legislative governance enforcing traceability within the manufacturing and assembly process.	External: Government compliance and political uncertainty	Nation state; Organization
Nation state control over foreign suppliers	External: Government compliance and political uncertainty	Nation state
Diminishing contribution of U.S. companies in technology standards bodies and open source software	Adversarial: Maintain a presence or set of capabilities.	Nation state

APPENDIX C: THREAT SCENARIOS

6.0 Threat Category: Counterfeit Parts

6.1 SCENARIO: SERVICE CONTRACTS

6.1.1 Background

Service contracts that are governed by the Trade Agreements Act (TAA) and Federal Acquisition Regulation (FAR) 25.1 sometimes include network equipment as part of the contract agreement (e.g., routers and switches).

6.1.2 Threat Source

This threat is applicable across any federal agency with these types of TAA service contracts that include network equipment.

6.1.3 Vulnerability

These network components are not required to have any engineering analysis or certification before installation on the network. Therefore, this is a network category threat with potential exposure to content data or other messaging.

6.1.4 Threat Event Description

Depending on the Original Equipment Manufacturer (OEM) or supplier, a change to TAA would require products to be authenticated or certified and meet specific engineering quality assurance.

6.1.5 Outcome

In this scenario, this threat could impact intellectual properties, network, data and messaging, depending on the contract. The exposure could be functional for an unspecified period of time.

6.1.6 Organizational Units / Processes Affected

Uncertain if there has been an impact. This example provides insight to a potential exposure.

6.1.7 Potential Mitigating Strategies / SCRM Controls

Possibly blockchain technologies may represent one mitigation strategy. Additionally, perhaps IoT systems used to monitor integrity of shipments from supplier to consumer. These may work for hardware supply chain. For software, there are mechanisms that include hashed or signed code along with blockchain, etc.

6.2 SCENARIO: ASSET MANAGEMENT, SPECIFICALLY SOFTWARE ASSET MANAGEMENT (SAM)

6.2.1 Background

A recent article from Gartner lays out the entire risk assessment with regard to asset management (specifically Software Asset Management (SAM). Agencies currently have many tools managing SAM such as IBM's Big Fix (HCL, an Indian company, is planning on buying a large part of IBM's Portfolio), SCCM (Microsoft), HP Universal Discovery, BMC's Remedy, Flexera and smaller agencies using spreadsheets. The significance of this dilemma is actually trying to capture spend analytics of SAM as the data models are different most everywhere and much of the data are unstructured. The solution is not to force all agencies to move to one tool but guide them to a structured data model and develop Application Programming Interfaces (API's) to pull the data on demand. Below, we discuss the technology and business risks associated with SAM within federal agencies, and the true spend numbers is and perhaps represent the usage of API's to gather full asset management. One more thing: SAM requires more than looking at installed instances. Usage data is critical to monitor and control SAM lifecycle, out-of-date software, and patch management.

6.2.2 Threat Source

N/A

6.2.3 Vulnerability

The business and technology risks are that agencies have different data models with each of these applications and therefore the accuracy of installed software, software utilization and outdated installed software (no longer supported) is not uncommon and can be of significant risk. Many agencies count instances of installed software but does account for software utilization. As an example, consultants often need Microsoft Visio Professional and Project Professional. There are many licenses installed without usage as we keep purchasing without measuring usage. Likewise, upgrades are not maintained appropriately (e.g., Adobe Acrobat and other Adobe products). Often the license expires and eventually no longer supported and therefore becomes an operational risk.

6.2.4 Threat Event Description

These network components are not required to have any engineering analysis or certification before installation on the network. Therefore, this is a network category threat with potential exposure to content data or other messaging.

6.2.5 Outcome

Sourcing, procurement and vendor management leaders working with IT asset managers to and risks should do the following:

- Develop a business case for Information Technology Asset Management (ITAM) to obtain cross-functional, C-level support for a published ITAM mission statement and charter that sets the foundation for IT asset life cycle governance;
- Design and implement comprehensive and formal controls to assign accountability for all activities across the IT asset life cycle. Assess current controls with stakeholders, and develop a roadmap to mitigate gaps in current controls;

- Implement organizational and operational governance boards that drive standardization and collaboration, provide role clarity, and support the ITAM initiative. This will minimize potential conflicts and objections to new policies and processes;
- Developing and implementing comprehensive IT asset life cycle controls is fundamental to the success of every ITAM initiative. Yet, when Sourcing, Procurement and Vendor Management (SPVM) and ITAM leaders are tasked with doing so, they struggle to know where to begin. They often overlook critical life cycle activities, or are unclear as to who is responsible for managing the steps of the life cycle. This lack of clarity results in inadequate controls that ultimately expose organizations to unwanted risks, such as software license noncompliance, unsecured assets, and uncontrolled costs;
- SPVM and ITAM leaders must develop and publish a mandate that is supported by cross-functional executives and driven by the ITAM strategy. The mandate should detail the activities in the IT asset life cycle and require the implementation of controls throughout the life cycle that account for the management of all IT assets (e.g., hardware, software, and cloud services). For the controls to be effective, ITAM policies, processes and leadership must be placed at the core of the IT asset life cycle to orchestrate and coordinate all life cycle activities; and
- The biggest challenge across federal is to develop a common data model for asset management. This does not warrant moving to a single application, but does require critical data management to be consistent and develop the applicable API's to pull data regardless of the installed application.

6.2.6 Organizational Units / Processes Affected

All agencies, sub-agencies, resellers, OEMs, and integration services could be affected by this threat. Depending on where this data is used elsewhere, it may possibly require changes to other applications and systems.

6.2.7 Potential Mitigating Strategies / SCRM Controls

The following mitigation strategies could be implemented:

- The opportunity will reflect in excess of 20 percent savings and cost avoidance opportunities;
- Asset management alignment with critical suppliers (initially) will significantly reduce risk and compliance issues regardless of platform (e.g., desktop, server, mainframe, cloud and security exposure);
- Meaningful financial reporting and forecasting;
- Quality spend analytics;
- System integrity; and
- Build an overall IT Asset Management Catalog by Platform and a process for maintenance.

6.3 SCENARIO: YOKOGAWA ELECTRIC CORPORATION COUNTERFEIT EQUIPMENT

6.3.1 Background

Yokogawa Electric Corporation identified instances in which several customers received counterfeit EJA-110E high-performance differential pressure transmitters used to measure liquid, gas, or steam pressure, using the Yokogawa logo.

6.3.2 Threat Source

The threat of counterfeit equipment labeled as OEM is applicable across federal, state & local agencies, as well as the critical infrastructure sectors that rely on these devices. The threats could occur outside OEM distribution paths at Integrators, third parties, etc.

6.3.3 Vulnerability

Vulnerabilities exist in a supply chain that includes system integrators, shippers, and other third parties. The threat is applicable at any time and persistent within the infrastructure.

6.3.4 Threat Event Description

Counterfeit instruments were produced by unauthorized manufacturers. In addition to a lesser quality, Yokogawa reports that performance test results found that the counterfeit products "pose a serious safety risk."

6.3.5 Outcome

In this scenario, this could impact intellectual properties, network, data, and messaging, depending on the contract. The exposure could be functional for an unspecified period of time.

6.3.6 Organizational Units / Processes Affected

There could be processes that impact the reseller or the integrator.

6.3.7 Potential Mitigating Strategies / SCRM Controls

N/A

7.0 Threat Category: Cybersecurity

7.1 SCENARIO: INCORRECT BORDER GATEWAY PROTOCOL (BGP) ROUTING

7.1.1 Background

BGP is the default protocol for exchanging routing information between Internet domains. Internet routing is designed to be resilient, and not dependent on any one organization. This presents a few inherent security problems that rely on trust of routing information. This inherent trust can make it harder to detect events such as route hijacking, route leaks, Internet Protocol (IP) address spoofing, eavesdropping, manipulation, and other harmful activities. BGP and other such routing threats can also be manifested by hackers who are not necessarily nation states, but also may be hacktivists or other non-state-affiliated actors. Route hijacking is when a route is accidentally or maliciously altered to send data traffic on an unintended route, or to an unintended destination. Further background information on BGP routing can be found here: https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/

7.1.2 Threat Source

The threat source in this scenario is a nation state, or other malicious actor that wishes to reroute or interrupt Internet traffic. Note that this threat can also manifest by accident. The impact will largely be the same, and the mitigations are also similar to malicious origins.

7.1.3 Vulnerability

Not all Internet Service Providers (ISPs) have implemented measures to ensure BGP announcements are coming from a legitimate source.

7.1.4 Threat Event Description

Users initially noticed a delay in certain Internet traffic. A traceroute that normally shows a route that takes two or three hops was now taking more than ten hops and also was routing via China. Further investigation shows

a colocation company leaked over 70,000 routes to a foreign Tier 1 provider. This provider then announced these routes on to the global Internet, which redirected large amounts of Internet traffic destined for some of the largest European mobile networks through China Telecom's network.

7.1.5 Outcome

The incorrect routes were in circulation for about one hour. During this time, traffic was routed thru China. This routing gave China the opportunity to collect intelligence from this traffic. Specific consequences of this intelligence breach are unknown. Once the incorrect routes were discarded, Internet routing traffic returned to normal.

7.1.6 Organizational Units / Processes Affected

All organizations that had traffic rerouted thru China were potentially impacted. For the Service Provider, Network Operations and configuration of border routers were affected.

7.1.7 Potential Mitigating Strategies / SCRM Controls

Organizations evaluating Internet Service Providers can inquire about policies and procedures, which are intended to prevent such occurrences, as well as monitoring that is intended to rapidly detect these events. The service provider can be asked if they are a member of the Internet Society's Mutually Agreed Norms for Routing Security (MANRS) project.

This threat scenario, is addressed in:

- Communications, Security, Reliability, and Interoperability Council (CSRIC) WG 3 -- Best Practices and Recommendations to Mitigate Security Risks to Current IP-Based Protocols
- National Institute of Standards and Technology (NIST) SP 1800-14, Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation

7.2 SCENARIO: RANSOMWARE ATTACK

7.2.1 Background

Ransomware is a type of malware where the target's computer is rendered unusable, typically by locking the user out of their system or encrypting some or all of the data on their system. The attacker then demands a monetary (bitcoin, etc.) ransom so that the target can receive the key to recover their data or access their system.

7.2.2 Threat Source

Ransomware attacks are typically propagated by individuals or groups seeking monetary gain.

7.2.3 Vulnerability

This threat is one of opportunity in that the threat actor sets their ransomware code afloat in the electronic sea – typically via infected web sites and email messages – waiting for an unsuspecting target to click on the link. While there are some antivirus packages which will recognize potential ransomware, the best defense is for users to avoid opening email messages from strangers, clicking on embedded links in email messages or visiting web sites for which there is not a personal or business need.

7.2.4 Threat Event Description

Ransomware has a variety of delivery vehicles or methods. These are three general examples of how ransomware can accomplish its goals.

In this example scenario, the threat actor is attempting to pose as a government official who is making final contact with the target to work out details of pending litigation or fines against the target. The generally worded email message contains a link and the target is instructed to click on the link to access the case file so that the target can avoid potential time in court and pending fines. Clicking the embedded link then unleashes the ransomware onto the target's computer.

In this example scenario, the target is presented with screen pop-ups which indicate that malware has been found on the target's system and the target should click on the link to take defensive measures. Again, clicking on the link unleashes the ransomware onto the target's computer.

In this final example scenario, the target has either turned off their antivirus software or configured it to its minimal settings thereby rendering it ineffective. As the target surfs the web, they can be presented with content which would normally have been flagged by their antivirus software. The target clicks on the questionable content and again unleashes ransomware onto the target's computer.

In each of the three example scenarios, above, there generally was not a named or intended target but rather just a wait-and-see who clicks on the infected link. Having said that, ransomware messages could be directed at organizations in general (companies, hospitals, government agencies) but again waiting to see if anyone will take the bait.

7.2.5 Outcome

If the threat actor is successful, the target is now presented with a dilemma; should they pay the ransom risking that the threat actor will not provide the key, or does the target attempt to recover their data from system back-ups, which could result in losing any data since the last back-up? Given that most times the ransom is to be paid using bitcoin or similar digital currency, the money leaves no audit trail.

If the target should pay the ransom, the threat actor could lock or encrypt the system again in the future seeking additional ransom payments. Most experts recommend that ransomware payments not be made, and the organization rebuild their system(s) from data back-ups.

7.2.6 Organizational Units / Processes Affected

Any and all parts of the organization are susceptible to ransomware attacks. Everyone who uses a computer, both professionally and privately, typically uses email and surfs the web, making everyone a potential target. Given the prevalence of outsourcing of supply chain activities, suppliers can be hit with ransomware as well thereby impacting a company's supply chain activities.

7.2.7 Potential Mitigating Strategies / SCRM Controls

While there is no single way to prevent ransomware attacks, strategies worth considering include:

- Regularly perform comprehensive backups of all critical data to offline or write-only storage on a schedule consistent with the number of transactions or data being performed on the system (e.g. how many days of data is the company willing to lose since the last back-up was performed?);
- Educate users on the potential perils of opening emails from strangers or clicking on embedded links (email or web sites);
- Keep anti-virus software active and up-to-date. Where possible, don't allow users to modify or disable anti-virus software on their company issued systems; and
- Contractual agreements should be in place with all suppliers to define liability and remediation activities should a supplier be impacted by a ransomware attack.

7.3 SCENARIO: REMOVABLE MEDIA ATTACK

7.3.1 Background

Threat Actors have utilized Removable Media to insert malware into an organization's computer systems. Removable Media such as Universal Serial Bus (USB) Thumb-Drives, Compact Discs (CDs), and floppy disks have been used. For examples of such methods and attacks see:

- Operation Buckshot Yankee: http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html
- Krebs On Security Article July 2018: https://krebsonsecurity.com/2018/07/state-govts-warned-of-malware-laden-cd-sent-via-snail-mail-from-china/

For organizations that do not have the appropriate security controls in place, when removable media is inserted into a computer, that system can look for executable files and attempt to run those programs. This can result in malware bypassing all network perimeter defenses and getting installed on systems inside the supply chain organization.

7.3.2 Threat Source

Nation state cyber threat actors have been behind the news worthy events of these removable media attacks. Cyber criminals or cyber hacktivists could also easily use this attack method.

7.3.3 Vulnerability

The vulnerability is that there is no prevention of, or pre-scanning of the malicious removable media prior to it being installed into the internal computer system. Removable media is delivered to an employee and that media is inserted into a computer system that can be compromised by that malware contained in or on the removable media.

7.3.4 Threat Event Description

When analyzing this threat scenario, the organization creates a fictitious, or potential, threat source described as a nation-state sponsored threat actor.

In this example scenario, the threat actor is attempting to compromise physical security systems being manufactured by the supply chain organization. The threat actor seeks to be able to remotely monitor and control the physical security systems of the supply chain organization's customers.

In this scenario, the threat actor drops many USB Drives, containing malware into the parking lot of the supply chain vendor. The USB Drives are labeled with supply chain organization's logo and the USB Drives contain file objects that appears to be related to the supply chain vendor's business.

Employees pick up the USB Drives, carry them into the organization. Many of the employees insert the USB drives into their computers. Some employees seek to return the USB Drives, some employees are curious about the USB drive contents.

In one study,[3] 48 percent of the distributed USB Drives were inserted into the organization's computers. Once inserted the computer can autorun the malware installation program. Or, the employee can attempt to open files, some with an alluring name, thus allowing the malware to start running, become installed, and open a backdoor so that the threat actor can access that system.

[3] https://www.pcworld.com/article/3070048/how-to-keep-usb-thumb-drive-malware-away-from-your-pc.html

When the threat actor has a persistent backdoor access to one of the supply chain vendor's systems, the threat actor can continue the attack.

7.3.5 Outcome

The threat actor is successful with their mission of compromising the systems being manufactured by the supply chain organization. The supply chain organization's customers are now buying systems that can be remotely controlled by the foreign military-intelligence organization. The supply chain organization is providing software updates to their existing customers, these updates contain the malicious capabilities. Depending upon the security controls in place within the customer's environment, the attacker is now able to remotely monitor and control the customers' entire physical security systems.

Additionally, the attacker now also has a foot hold in each of the supply chain organizations customer's networks. This can enable the attacker to launch additional attacks into each of those organizations.

7.3.6 Organizational Units / Processes Affected

The supply chain organization is compromised, the attacker has the ability to move freely within their network and systems. The company's products have been compromised; therefore, their customers are also potentially affected. The compromised physical security system is now a platform from which the attacker can begin to attack each organization where their security system in installed.

7.3.7 Potential Mitigating Strategies / SCRM Controls

The buyer organization, conducting this analysis, would evaluate:

- The extent to which potential supplier organizations protect themselves from removable media type attacks;
- The extent to which the organizations are connected electronically;
- The extent to which the supply chain organization has mature security-focused software development and distribution practices; and
- Internal security controls, such as micro segmentation, so that such a compromised system would not be able to communicate outside of the organization.

This threat scenario, removable media, is addressed in:

- NIST Special Publication (SP) 800-53 Rev 4 Security Control: Media Protection.
- NIST SP 800-161 [Supply Chain Risk Management Practices for Federal Information Systems and Organizations] references NIST SP 800-53 Rev 4 Security Control: Media Protection.

7.4 SCENARIO: RESOURCE DEPLETION – UNINTENTIONAL/ACCIDENTAL SHUTDOWN

7.4.1 Background

Unintentional or accidental resource depletion is a non-adversarial threat resulting from system misconfigurations or lack of resource planning. System events resulting in resource depletion or accidental shutdown may vary from misconfiguration of information systems and network connectivity to improper software updates to production environments.

Organizations operating without the appropriate security controls in place will experience regular system and network outages inadvertently caused by uncontrolled and unmanaged changes to their environments. This will cause a reduction in the organizations overall systems and network availability.

7.4.2 Threat Source

The threat source in this scenario is internal and is also non-malicious.

7.4.3 Vulnerability

The vulnerability is the lack of, (or lack of enforcement of) change management and configuration management policies and procedures within the organization.

7.4.4 Threat Event Description

When analyzing this threat scenario, the organization creates a fictitious, or potential, threat source described as an internal employee with non-malicious intentions.

In this scenario, the supply chain organization recently hired a new network engineer who identified some inefficiencies in the existing network configurations. The network engineer updates the system routing configurations and applies the updates to the production network without recording the updated configurations.

7.4.5 Outcome

The internal employee unintentionally caused an accidental shutdown crippling the supply chain organization's enterprise creating a negative impact on the supply chain organization and possibly their client organizations.

7.4.6 Organizational Units / Processes Affected

The supply chain organization may experience productivity inefficiencies caused by system or network outages possibly impacting their ability to support or deliver on their contracts. The supply chain organization's customers may also experience impacts to their existing operations through system, service availability, or product supply.

7.4.7 Potential Mitigating Strategies / SCRM Controls

The buyer organization, conducting this analysis, would evaluate:

- The presence of Configuration Management policies and procedures that are in place and actively enforced;
- Assess the overall impact of vendor system or network outages will have on the organizations operations; and
- Assess the overall impact of vendor system or network outages will have on the vendors' ability to meet contractual requirements.

This threat scenario, Resource Depletion/Unintentional Shutdown, is addressed in:

- NIST SP 800-53 Rev 4 Security Controls: Configuration Management, System and Information Integrity
- NIST SP 800-161 [Supply Chain Risk Management Practices for Federal Information Systems and Organizations] references NIST SP 800-53 Rev 4 Security Control: Configuration Management, and System and Information Integrity.

8.0 Threat Category: Internal Security Operations and Controls

8.1 SCENARIO: POOR ACCESS CONTROL POLICY

8.1.1 Background

An organization has a small legacy network, which has been maintained over a period of 10+ years but has not been assessed for risk or security threats in quite some time. The network is mostly static in nature, in both configuration and system level/type (OS, patch, function, applications, etc.). Over that period, the team responsible for monitoring and managing the security of this network has changed several times, with no update or re-check of policies and procedures.

The organization has decided to perform some routine network checks prior to upgrading other portions of the infrastructure and has called in a pre-existing vendor to verify systems and configurations.

8.1.2 Threat Source

The systems involved are part of legacy wireless infrastructure which still routes traffic in certain areas and is also available as fallback for emergency or backup situations.

While the current infrastructure has been through audits and assessments over time, the legacy infrastructure has largely been signed off as status quo.

8.1.3 Vulnerability

While the network routes a relatively small amount of traffic, it does have access to a large amount of subscriber information that is maintained for the current infrastructure. The systems control access to sensitive user data, Domain Name System (DNS) function and routing of user traffic in, out, and through the legacy network.

8.1.4 Threat Event Description

Due to weak access control policies, years-old user accounts from the equipment vendor are still functional. Some of these user accounts allow root or privileged access and are not uniquely identifiable as belonging to an individual or even to a certain company. The credentials for these accounts have become compromised and a malicious attacker has used them to gain access to the legacy network, where additional attacks can be sourced from.

8.1.5 Outcome

The following illustrates some of the weaknesses exposed in an attack chain that could be sourced from this supplier:

- Some equipment is accessible directly from the enterprise network, not via a firewall or Demilitarized Zone (DMZ);
- User accounts are not uniquely identifiable, reviewed or changed;
- User sessions are not controlled and vulnerable to typical brute force account access methods; and
- Potential violations of user access are not alerted.

Given the above factors, an attack would not only likely be successful but also would go undetected for a long time unless service was otherwise impacted (e.g. user traffic stopped passing or was degraded). Simple dictionary or brute force attacks would likely be successful due to access control and account management policies. Thus, theft or manipulation of data, either through man-in-the-middle or exfiltration would be quite

possible. In addition, other defenses or mitigations set up elsewhere in the network could be negatively impacted or changed from within.

8.1.6 Organizational Units / Processes Affected

N/A

8.1.7 Potential Mitigating Strategies / SCRM Controls

Proper access control means protection of system resources against unauthorized access; a process by which use of system resources (e.g. executable programs, network configuration data, application file systems, network databases etc.) is regulated according to a security policy and is permitted only to authorized entities (users, programs, processes or other systems) according to that policy.

Authentication and authorization are basic security methods, which provide means to ensure the identity of users and limit their use of network resources to predefined activities or roles. They can thus be used to protect network operators against any unauthorized use of the network's services.

Furthermore, user authentication provides a basic mechanism for logging and auditing the management activities, which makes it possible to track activities afterwards. Providing each user with a unique user Identification (ID) and password together with a certain profile (privilege level) makes it possible to limit user's access to only those management activities they require in order to perform their task.

Enforcing the strong password selection, password aging (which enforces the users to change their passwords at predefined intervals), two-factor authentication, and the encryption of the files containing the user ID and password data (to prevent unauthorized users to obtain sensitive data) provide additional security.

It is also recommended to implement restrictions on the rate of login attempts, concurrent login attempts, and lockout periods for incorrect login attempts and monitored alerts for incorrect login attempts.

Security event logs or audit trails are of fundamental importance to an operator in detecting malicious activities by defining the indicators of such behavior. The log also establishes accountability for malicious users committing internal fraud or sabotage. The security event logging should be compliant to open standards to permit the administrator to perform archival and analysis of logs and for post-incident evidence gathering and investigation.

The first step to detect harmful activities is to know the indicators for such behavior. The earlier such an activity is detected, the more time is left to take appropriate countermeasures.

8.2 SCENARIO: DEVICES THAT DON'T AUTO-UPDATE FIRMWARE (IMBEDDED SPINAL CORD STIMULATOR WITH A HAND-HELD CONTROLLER)

8.2.1 Background

Failing to update your software doesn't just mean you won't have the latest version, it means you could be exposed to major security vulnerabilities that could also affect your physical wellbeing. There's medical technology today that allows patients to control their comfort levels by carrying a hand-held device to monitor and control implantable medical devices. After numerous, unsuccessful surgeries, a patient received a surgically implanted spinal cord stimulator to address years of chronic back pain. The stimulator tricks the brain to thinking the pain is gone.

8.2.2 Threat Source

The unauthorized individuals potentially accessing the device and changing the setting that control and monitor the comfort level of a patient. The hacker could turn the controller completely off making it impossible

for the patient to active the device and receive the benefits provided by the device to manage pain. As defined - a threat is the potential for a threat source to successfully exploit a vulnerability.

8.2.3 Vulnerability

Hand-held devices don't auto-update and requires live conversation with a help desk and, in some instances, a trip to the patient's health care provider must take place to update the firmware and sync the device.

8.2.4 Threat Event Description

Unauthorized individuals accessing the device and changing the settings that control/monitor the comfort level of a patient. The hacker could turn the controller completely off making it impossible for the patient to activate the device and receive the benefits provided by the device to manage pain. Conversely, the hacker could turn the controls up or down making the pain encountered by the patient intolerable.

8.2.5 Outcome

Since it doesn't appear to allow hackers to gain access to a patient's medical/personal history, the primary threat is controlling the device itself, which is some instances where the imbedded device may be something other than a spinal cord stimulator (i.e. pacemaker) could be life altering.

8.2.6 Organizational Units / Processes Affected

N/A

8.2.7 Potential Mitigating Strategies / SCRM Controls

- To mitigate the seriousness of such an attack, patients who have an imbedded device that require updates from time to time should ensure that their contact information is kept up to date with the manufacturer of the medical device, as well as their health care providers so that the patient can be notified when an update to a device is required;
- Periodically, contact the manufacturer of the device for firmware updates; and
- Make regular appointments with healthcare provider to ensure the device is working properly.

8.3 SCENARIO: MISHANDLING OF CRITICAL OR SENSITIVE INFORMATION

8.3.1 Background

An energy company supplier, Griffon Power, routinely handles marketing and technical information on industrial components used throughout their network. These are sometimes internal in nature but are generally marked as such. Recently, a small team within the company reviewed confidential external information from a domestic supplier on parts that were proposed for new turbines. These documents were highly sensitive in nature and shared under a Non-Disclosure Agreement (NDA).

8.3.2 Threat Source

As part of the project analysis, the team set up a shared network drive to distribute and review information. All information related to the project was stored within this folder, which was only accessible internally. Griffon Power ultimately decided not to go forward with the new turbine offering and moved on with other business. About a year later, as part of a network cleanup and upgrade effort, network storage was decommissioned and sold off to an offshore company for parts.

Much of the NDA-level information shared between Griffon Power and the potential supplier has not been properly handled and is now exposed to a third party company.

8.3.3 Vulnerability

Not having a process, to properly decommission network storage which was eventually sold off to an offshore company for parts.

8.3.4 Threat Event Description

Proprietary information on the inner workings and specialty parts of turbines that are used throughout energy companies has been made available and sold on the dark web. This could be used for economic or blackmail purposes or by foreign competitors to gain an unfair advantage in the market.

8.3.5 Outcome

Some of the weaknesses exposed in Griffon Power's policies on the handling of data are:

- Failure to wipe data that is no longer used;
- Failure to classify data – then handle and protect according to the classification;
- Failure to implement document-level encryption for sensitive data; and
- Failure to audit systems prior to decommissioning.

8.3.6 Organizational Units / Processes Affected

N/A

8.3.7 Potential Mitigating Strategies / SCRM Controls

Data management policies can have a broad range of useful steps that could prevent such risks in this scenario. All data should be classified according to its intended use, who is allowed to access it, and if or how it can be shared. In addition, data tags could be set according to whether it is Public, Limited Release, Internal or Confidential (for example). Depending on how the data are classified, it may need to be encrypted and have access to the data controlled and monitored.

Separately, companies should have a process and policy for decommissioning equipment and perform regular audits before any such equipment is released, sold or distributed. At a minimum, any non-Public data should be removed from any systems; in most cases, it is advisable to perform a complete wipe of data or destruction of storage devices to a sufficient level that data cannot be recoverable later.

8.4 SCENARIO: LACK OF ASSET VISIBILITY AND VULNERABILITY EXPLOITATION

8.4.1 Background

An organization in the supply chain lacks visibility into the range and numbers of assets connecting to its network. Further, this organization only scans for vulnerabilities on an annual basis, as part of a compliance requirement. The organization also fails to plan and prioritize its vulnerability mitigation practices.

8.4.2 Threat Source

Many high-profile incidents, including the Equifax breach and WannaCry, could have been prevented through better cyber hygiene. Fifty-seven percent of enterprises that experienced a breach in the past two years state that a known, unpatched vulnerability was the root cause.[4]

[4] "State of Security Response," Ponemon/ServiceNow, 2018

The discovery and disclosure of vulnerabilities continue to grow in volume and pace. In 2018 alone, an average of 45 new vulnerabilities were published every single day, for a total of 16,500, up from 15,038 in 2017.[5]

With 59 percent of all vulnerabilities in 2018 rated as Critical or High severity, security organizations are challenged to determine which vulnerabilities truly represent a risk and prioritize the most critical vulnerabilities to maximize limited remediation resources. After all, the proportion of Common Vulnerabilities and Exposures (CVEs) with a publicly available exploit was seven percent in 2018, down one percentage point from 2017.

8.4.3 Vulnerability

The vulnerability in the scenario is that the organization in the supply chain lacks visibility into the range and numbers of assets connecting to its network.

8.4.4 Threat Event Description

As more devices are connected, the attack surface expands, often in unexpected places, such as building management systems and Close-Circuit Televisions (CCTVs). These systems perform multiple functions, such as managing access to specific doors, controlling door alarms, creating the photo IDs that allow facility access and monitoring for access.

Coupling together three vulnerabilities in the past year, an attacker could setup a Zoom video conference with any target at the organization. Once connected, the attacker can control the attendee's screen by exploiting a vulnerability in Zoom[6] allowing them to download and install malware on the target's computer.

With access to the target computer, the attacker can then exploit the building management system[7] allowing physical access to the building. Now that the attacker can access the facility, the last step is to ensure the CCTV does not record their intrusion by exploiting the CCTV system.[8] In this scenario, an attacker could exploit software vulnerabilities to gain administrator rights, enabling them to create fraudulent ID's, disable door locks and alarms, access sensitive authorized user data and delete video footage.

8.4.5 Outcome

Building management contractors, just like IT managers, must consider cyber risk associated with all computer systems and networks within their scope of responsibility. Often times, building management systems and CCTV are outside the control or purview of organization IT departments. A disciplined Vulnerability Management program, by which the organization can track, assess, and remediate known vulnerabilities across their entire attack surface in a timely manner, before they can be exploited is a must.

8.4.6 Organizational Units / Processes Affected

N/A

8.4.7 Potential Mitigating Strategies / SCRM Controls

- Identify business operations and assets most vulnerable to cyber-attacks, to include third party, Operational Technology (OT) and IoT assets; for many organizations, the most critical assets are those that have the highest monetary value attached to them; for the government, this may be those deemed most mission critical;

[5] Primary Research, Tenable Vulnerability Intelligence
[6] https://www.tenable.com/press-releases/tenable-research-discovers-vulnerability-in-zoom-that-could-lead-to-conference
[7] https://www.tenable.com/blog/multiple-zero-days-in-premisys-identicard-access-control-system
[8] https://www.tenable.com/press-releases/tenable-research-discovers-peekaboo-zero-day-vulnerability-in-global-video

- Utilize continuous threat intelligence to prioritize remediation efforts in light of the overwhelming number of new vulnerabilities; organizations should use contextual factors including asset criticality and whether there are exploits available for specific vulnerabilities, in prioritization;
- Frequent scanning and reporting is critical, because out-of-date data can be just as damaging as inaccurate data. The Center for Internet Security (CIS) Control 3.1 recommends automatically scanning all systems on a weekly or more frequent basis;
- Organizations need to make sure their reporting is aligned with their patch remediation cycle so that reporting and updates are relevant;
- Identify the security gaps and opportunities to reduce complexity in the IT security infrastructure that leave organizations vulnerable to cyber-attacks;
- Measure the value of responding to vulnerabilities through automation and machine learning; and
- Utilize IT security staff and resources to improve the efficiency of vulnerability management.

8.5 SCENARIO: ICT DEVICES WITH DEFAULT PASSWORDS

8.5.1 Background

All ICT devices ship with default passwords, not changing the administrator password can result in the attacker to easily identify and access ICT systems. It is imperative to change default manufacturer passwords and restrict network access to critical and important systems.

8.5.2 Threat Source

One of the first things a hacker checks is whether the default account and password are enabled on a device. Websites such as www.defaultpassword.com list the default credentials, old and new, for a wide variety of devices:

- Routers, access points, switches, firewalls, and other network equipment
- Databases
- Web applications
- Industrial Control Systems (ICS) systems
- Other embedded systems and devices
- Remote terminal interfaces like Telnet and SSH
- Administrative web interfaces
- ERP systems

In 2014, Trustwave released the results of an analysis of 691 data breaches and concluded that one third were due to weak or default passwords. In 2018, it was reported that less than 8 percent of analyzed breaches were due to weak or default credentials. While the trend suggests that password security is improving, it remains crucial to have a process in place for dealing with new equipment which may still be configured with the manufacturer's passwords.

8.5.3 Vulnerability

Devices ship with default passwords, not changing the administrator password can result in the attacker to easily identify and access ICT systems. It is imperative to change default manufacturer passwords and restrict network access to critical and important systems.

8.5.4 Threat Event Description

A small ISP has been breached by an attacker that has gained access to the enterprise network through a router with the factory default password.

8.5.5 Outcome

The attacker with knowledge of the password and network access to a system can log in, usually with root or administrative privileges. Further consequences depend on the type and use of the compromised system. Examples of incident activity involving unchanged default passwords include:

- Internet Census 2012 Carna Botnet distributed scanning;
- Fake Emergency Alert System (EAS) warnings about zombies;
- Stuxnet and Siemens SIMATIC WinCC software;
- Kaiten malware and older versions of Microsoft Standardized Query Language (SQL) Server;
- Secure Shell (SSH) access to jailbroken Apple iPhones;
- Cisco router default Telnet and enable passwords; and
- Simple Network Management Protocol (SNMP) community strings.

8.5.6 Organizational Units / Processes Affected

N/A

8.5.7 Potential Mitigating Strategies / SCRM Controls

- To reduce the risk of security breaches through default credentials which have been left configured on network devices, it's best to implement a process to change the passwords, and if possible account names, when new equipment is installed.
- Identify software and systems that are likely to use default passwords. Regularly perform vulnerability network scans to identify systems and services using default passwords. Additionally, utilize good password management including:
    - Change Default Passwords - Change default passwords as soon as possible and absolutely before deploying the system on an untrusted network such as the Internet. Use a sufficiently strong and unique password. See the United States -Computer Emergency Readiness Team (U.S.-CERT) Security Tip ST04-002 and Password Security, Protection, and Management for more information on password security;
    - Use Unique Default Passwords - Vendors can design systems that use unique default passwords. Such passwords may be based on some inherent characteristic of the system, like a Media Access Control (MAC) address, and the password may be physically printed on the system;
    - Use Alternative Authentication Mechanisms - When possible, use alternative authentication mechanisms like Kerberos, x.509 certificates, public keys, or multi-factor authentication. Embedded systems may not support these authentication mechanisms and the associated infrastructure;
    - Force Default Password Changes - Vendors can design systems to require password changes the first time a default password is used. Recent versions of DD-WRT wireless router firmware operate this way; and
    - Restrict Network Access - Restrict network access to trusted hosts and networks. Only allow Internet access to required network services, and unless absolutely necessary, do not deploy systems that can be directly accessed from the Internet. If remote access is required, consider

using Virtual Private Network (VPN), SSH, or other secure access methods and be sure to change default passwords.

- Vendors can design systems to only allow default or recovery password use on local interfaces, such as a serial console, or when the system is in maintenance mode and only accessible from a local network.

8.6 SCENARIO: INCORRECT PRIVILEGE SETTINGS, AUTHORIZED PRIVILEGED USER, OR ADMINISTRATOR ERRONEOUSLY ASSIGNS USER EXCEPTIONAL PRIVILEGES OR SETS PRIVILEGE REQUIREMENTS ON A RESOURCE TOO LOW

8.6.1 Background

Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.

8.6.2 Threat Source

Access controls that define specific sets of privileges linked to individuals are a fundamental security practice. However, these same principals are not always applied to the most sensitive access of all; high-privilege access administrative accounts that have massive control over business-critical IT functions.

High-privilege access may be the most sensitive aspect of IT. Administrative accounts have the ability to make widespread changes to IT systems on which the business may depend. If misused, these capabilities can cause extensive damage ranging from security threats and compliance violations to incidents that tarnish the reputation of the business itself.

8.6.3 Vulnerability

The vulnerability is that the company until recently had no formal Information Security Policy or related procedures. There has been no policy for assigning system privileges, leading to many users having administrative or super user system privileged access which are not required for their current job. In this scenario, a user was granted root access to a UNIX system, in which the operating system does not apply access controls to the user root. That user can terminate any process and read, write, or delete any file.

8.6.4 Threat Event Description

Acme Packet is a midsized manufacturing company which has doubled its enterprise product offering and number of employees. When the company first started, it had less than 25 employees, many of which had multiple responsibilities. One example includes the office manager also serving as their IT department. Additionally, the company until recently had no formal Information security policy or related procedures. There has been no policy for assigning system privileges, leading to many users having administrative or super user system privileged access which are not required for their current job.

In this scenario, a user was granted root access to a UNIX system, in which the operating system does not apply access controls to the user root. That user can terminate any process and read, write, or delete any file.

8.6.5 Outcome

The scenario above presents multiple risks to the supply chain ranging from insider risks to cyber espionage. Additionally, the easiest way for a cyber-attacker to gain access to sensitive data is by compromising an end

user's identity and credentials. Things get even worse if a stolen identity belongs to a privileged user, who has even broader access, and therefore provides the intruder with *the keys to the kingdom*. By leveraging a *trusted* identity, a hacker can operate undetected, gaining access to sensitive data and system access with little or no indications to the attack.

8.6.6 Organizational Units / Processes Affected

N/A

8.6.7 Potential Mitigating Strategies / SCRM Controls

- Conduct a security review of all users physical and system access adjusting user access to least privileged access, the minimum access needed to perform the job.
- Establish an Information Security Policy based off industry standards and best practices
- Deploy and Privileged Access Management (PAM) system for monitoring and protection of super user accounts. This is one of the most important aspects of Identity and Access Management, and cybersecurity at large today. With a PAM solution in place, an organization can dramatically reduce the risks discussed above.
- The Best Practices for Privileged Access Management utilize the Four Pillars of PAM. Gartner outlines key challenges and makes clear recommendations that emphasize the critical role of people, processes and technology in effectively mitigating PAM risk and making purchase decisions, including:
  - Track and Secure Every Privileged Account;
  - Govern and Control Access;
  - Record and Audit Privileged Activity; and
  - Operationalize Privileged Tasks.

9.0 Threat Category: Compromise of System Development Life Cycle (SDLC) Processes & Tools

9.1 SCENARIO: MANIPULATION OF DEVELOPMENT TOOLS & DEVELOPMENT ENVIRONMENT

9.1.1 Background

Both hardware (printed circuit boards and computer chips) and software (source or object code and firmware) are highly reliant upon automated development tools. A Printed Wiring Board (PWB) (the circuit board to which components are soldered) is composed of hundreds, if not tens of thousands of circuit traces and component connections. A much smaller instance of this is the computer chip which can contain thousands of transistors and other elemental circuit components. Likewise, on the software side, computer code in its source form can constitute thousands or millions of lines of instructions, and often integrates dozens of third-party components. Once compiled, this can reach megabytes of binary code.

Given the complexity of both hardware and software development processes, threat actors may seek to introduce vulnerabilities into the hardware or software through development processes or tools, or by compromising the development environment.

9.1.2 Threat Source

Manipulation of development tools and development environments can come by way of a variety of different threat actors: nation state, organization or individual (outsider or insider).

9.1.3 Vulnerability

The threat actor may use the complexity of the hardware or software itself (thousands of circuit traces or lines of source code) to help cover their tracks. If the development environment is not set up and managed correctly with all developers observing the accepted organizational rules-of-the-road and adopting secure configurations and controls, threat actors can use the complexity to their advantage (e.g. lax check-out check-in procedures, non-existent or minimal revision processes, unprotected code repositories, etc.). Misconfigured or unpatched anti-virus software was unable to detect the infected software running the factory machines implanted from the USB drive.

9.1.4 Threat Event Description

When analyzing this threat scenario, the organization creates a fictitious, or potential, threat source described as an individual threat actor in the first case and a nation state in the second case.

In this example scenario, the threat actor is a hardware Research & Development (R&D) engineer of the company. He or she reconfigures a computer-assisted design (CAD) system so that he or she can work remotely from home. The company's IT department was not consulted when a hole was created in the company firewall. While the employee was well-intentioned and took it upon him or herself to do the work, a vulnerability has now been introduced into the company.

Additionally, in this example scenario, the threat actor is a rogue nation state. After surveilling the target company via the Internet for some time, the threat actor has found an unpatched vulnerability allowing remote access to the company's development environment housing source code. The threat actor can now decipher the source code to learn the inner workings of a particular product, thereby stealing the Intellectual Property (IP*) for their own use or profit.

9.1.5 Outcome

In the first scenario, the well-intentioned employee has created a vulnerability in the development tools which is just waiting to be exploited by a bad actor (nation state, organization or individual). The vulnerability is eventually exploited, and the company finds itself under attack.

In the second scenario, not keeping systems patched and knowing where vulnerabilities can exist has led to the company's IP* being stolen, thereby leading to a company's loss of market share and dominance in a particular market sector.

9.1.6 Organizational Units / Processes Affected

In both of these scenarios, the company who owns the development tools and the development environment is directly impacted. R&D and manufacturing operations both rely upon the development tools and associated development environment for the data they contain. If IP* has been stolen, long term viability of the company may be at stake.

9.1.7 Potential Mitigating Strategies / SCRM Controls

Preventing the manipulation of a company's development tools and development environment can benefit from the following:

- Access controls and identity and authentication management controls must be in place for all development tools (hardware and software) and for the broader development environment. Only those people with a need to access the tools and data should be granted access, no more. When appropriate, enforce segregation of duties on hardware or software projects such that a developer (hardware or software) can only access their particular area of the design. Where possible, use identity management and change management tools to track changes made to the project;

- Providing external access (outside the company firewall) to any tools or data must be done in coordination with the IT department or equivalent function within the company;
- Keep all system and tool patches up-to-date; and
- Observe good SDLC practices in the development environment (check-out check-in, revisions, etc.) and remove old code when it is no longer needed.

9.2 SCENARIO: COMPROMISED/INFECTED SYSTEM IMAGES

9.2.1 Background

To gain economies of scale, electronic products are typically assembled and programmed on an assembly line. In this case, the first unit looks like the second unit, which looks like the nth unit. One down side to this approach is that when infected code is found in one unit (infected via software download to rotating media, embedded firmware, etc.), ALL units will contain this infected code. Having compromised or infected system images on the factory floor can become a huge problem for the manufacturer.

9.2.2 Threat Source

Compromise or infection of system images can come by way of a variety of different threat actors: nation state, organization or individual (outsider or insider).

9.2.3 Vulnerability

The working assumption on the factory floor is that everything is good until an issue is discovered. Automated hardware test systems can be quite adept at finding hardware issues (parts out of spec/tolerance, parts loaded incorrectly, wrong speed grade of parts used, etc.). What is more elusive is the ability of the factory floor equipment to find compromised or infected software. Hardware can be touched and physically examined. Software is 1's and 0's and must be examined using software tools which have been tuned to look for specific flaw, compromise, or infection…a more challenging task!

9.2.4 Threat Event Description

When analyzing this threat scenario, the organization creates a fictitious, or potential, threat source described as an individual threat actor.

In this example scenario, the threat actor is an external actor who develops and distributes malware implanted on a desktop Personal Computer (PC). A hardware engineer responsible for products being manufactured on the adjacent factory floor inserts a USB thumb drive into his or her desktop PC, copies some required files onto the drive and removes it from the PC. The engineer then enters the factory floor where he or she inserts the thumb drive into one of the factory floor control systems.

Unknowingly he or she has transferred a virus from the desktop PC to the factory floor. The virus, which may include code enabling the threat actor to manipulate or sabotage an infected product, now finds its way onto the product flowing down the manufacturing line. Soon those infected products are shipped to customers around the world.

9.2.5 Outcome

After the product is delivered to the customer, they turn on the new piece of equipment, the customer then runs an anti-virus program only to discover the new unit is infected. The customer contacts the manufacturer, demanding why they are receiving infected product. This puts the manufacturer into emergency mode with all hands on deck to track down the source of the virus…is this a one-off situation? Are other customers seeing this issue? Was the product tampered with in route to the customer? Many questions need to be answered in very short time!

9.2.6 Organizational Units / Processes Affected

While the end user customer is the first to be impacted with a compromised or infected system image, ultimately it is the manufacturer who bears the brunt of the impact. The two questions that need immediate answering are *how* and *where* was the code compromised or infected? Once that is determined, the conversation then turns to mitigation strategies to prevent further compromise or infection and how to address all the units currently in other customers' hands which contain the same compromise or infected system image (this includes any potential announcement to be made to the press). These will be all hands on deck activities from both R&D engineers and the factory floor team.

9.2.7 Potential Mitigating Strategies / SCRM Controls

There is no single method of preventing compromised or infected system images from finding their way on the factory floor. Prevention strategies should include the following:

- Use hashes or other analytical tools to confirm that the system image on the factory floor master system has not been changed/compromised. Depending upon the effort involved, this should be performed at least once daily; before and after each shift would be preferred;
- Create a list of all files required on the customer product. Periodically check the file content of the factory floor systems against this list to ensure additional files have not been placed on the factory floor system. These additional files could cause serious issues once the equipment is installed at the customer site;
- Restrict the use of USB thumb drives and other removable media on the factory floor. If removable media must be used (either to move information onto or off of the factory floor or as part of the manufacturing process), purchase the media from reputable suppliers. Scan the removable media with anti-virus software when entering and leaving the factory floor;
- System images can be compromised or infected by other methods, such as a threat actor accessing the factory floor systems via an unpatched system or network vulnerability;
- Ensure all system and network patches are installed and anti-virus software is up-to-date;
- Ensure that appropriate physical access controls are in place for the factory floor. The factory floor should be accessed only by those individuals who have need to do so; and
- Ensure that any new or updated system images being loaded onto the factory floor manufacturing systems have been thoroughly scrubbed to ensure viruses are not present in the code or file set.

9.3 SCENARIO: INTRODUCTION OF VULNERABILITIES INTO SOFTWARE PRODUCTS FROM OPEN SOURCE

9.3.1 Background

Modern software development practices often involve the integration of open source components into a larger piece of software, and complex software products or services may integrate dozens or even hundreds of such components. Open source libraries provide developers with ready-made, community-vetted code to perform discrete functions used in larger software products and services. As such, open source code can be a huge time saver for any programmer who is typically faced with seemingly impossible development deadlines. In some cases, the use of open source code can significantly reduce software development times.

9.3.2 Threat Source

Vulnerabilities introduced by the use of open source code are typically done by individual actors, but can also be introduced by organization or nation-state actors.

9.3.3 Vulnerability

The very nature of open source code is that anyone can typically view and manipulate the source code to meet their needs (some licensing requirements may apply). Given this openness, peer review is relied upon to keep the code clean and free of malware. An experienced and determined software engineer could hide a few lines of malicious code in the open source, intending that it goes unnoticed.

9.3.4 Threat Event Description

When analyzing this threat scenario, the organization creates a fictitious, or potential, threat source described as an individual threat actor.

In this example scenario the threat actor injects a few lines of malicious code into some commonly used open source code. A software project team, under severe time constraints, picks up and uses the infected open source code and the development team's tools for vetting and testing the component do not detect the malicious code. Unknowingly they have introduced a vulnerability into their software code.

9.3.5 Outcome

The vulnerability has gone undetected in the software team's code and the threat actor is able to compromise the software through the inserted vulnerability. The resulting effect on the code and ultimately the end customer can take a variety of forms, from being annoying to impacting system performance to the loss of data.

9.3.6 Organizational Units / Processes Affected

The end user customer is directly impacted in whatever way the injected code manifests itself. Since much of the open source code is ultimately compiled into larger pieces of code, it will be difficult for the customer to isolate and eliminate the issues introduced by the rogue code.

Once reported to and isolated by the manufacturer, eliminating the problem code will require recompilation of the source code and distribution to the customers, assuming the customers are able to download the updated object code.

9.3.7 Potential Mitigating Strategies / SCRM Controls

Strategies to help prevent the unintended introduction of vulnerabilities when using open source code include:

- Performing open source peer code reviews to help ensure the open source code is clean;
- Subject all third-party components to common software and security testing tools and practices;
- Maintain a protected source code library of pervious pieces of open source code which have been vetted and approved for use in the company. Keep the source code files up-to-date with any patches which have been issued in the open source community for that particular file. Use file integrity tools to ensure the code library is not tampered with.
- Observe all SDLC practices involving open source code. The code is only as strong as its weakest link. Cutting corners to save time or stay on schedule could cost dearly later; and
- Monitor open source vulnerability news and keep open source libraries patched and up-to-date.

10.0 Threat Category: Insider Threat

10.1 SCENARIO: CONTRACTOR COMPROMISE

10.1.1 Background

Nation-state threat actors have always utilized people to help them conduct their intelligence gathering operations. In some cases, they attempt to infiltrate people into an organization. In other cases, the threat actors attempt to compromise people already working at the organization of interest. These people might be employees or onsite contractors. In another aspect, corporate espionage by competitors can be effected via an insider.

Additionally, there are non-nation-state, ideologically driven, organizations that attempt to recruit individuals that could be onsite contract employees.

The risks presented by this type of attack are compounded when organizations outsource some of the work that needs to be accomplished. The risk is compounded because often it's the company that is hired that is screening the employees that will be onsite performing the work.

This sample threat scenario is the case where an onsite IT contractor employee is compromised, or recruited, by a threat actor and becomes an insider threat.

This scenario will not address all of the potential negative actions the insider could take. This scenario will focus on mitigating the chances that such a compromised insider, from the supply chain, can remain undetected once the compromise takes place.

10.1.2 Threat Source

The threat source, in this example, is an onsite contract employee that becomes compromised, or recruited, by a threat actor. The contract employee then becomes an onsite tool of the threat actor.

10.1.3 Vulnerability

The vulnerability in this example is the inability to detect that an employee has become compromised, or recruited, by a threat actor.

10.1.4 Threat Event Description

A full-time contract employee is providing IT Services to an enterprise. The enterprise is the target of the threat actor. The threat actor may wish to steal, change, destroy, or hold hostage data or the threat actor may wish to disrupt operations, or corrupt or sabotage a product.

The relevant threat event is the successful recruitment of the contractor individual and the fact that the individual then attempts to undertake the malicious activity.

10.1.5 Outcome

The outcome is an undetected malicious insider that is a contract IT employee, coupled with activity that the undetected malicious insider undertakes.

10.1.6 Organizational Units / Processes Affected

The affected organization is the organization that has the onsite IT Contractor working within their environment. Depending upon the specific bad activity, other potential impacts could occur for other business partners of the enterprise.

10.1.7 Potential Mitigating Strategies / SCRM Controls

The potential mitigating strategies would be an element of the Risk Management Process as described by the Risk Management Framework. See the following for more information: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

Potential Mitigating Strategies could include:

- Contractually requiring contractors to have the same background and periodic security check that employees must conform to. Additionally, the contractor company would be required to share the results of these checks with the buyer or hiring organization.
- Delivering insider awareness training to enterprise employees, and contractors, would better enable the insider-contract-employee to be identified.

10.2 SCENARIO: NEW VENDOR ONBOARDING

10.2.1 Background

Reaching out to new semiconductor companies can give manufacturers a performance or pricing edge, especially when the market has lean margins to work from and compete for government contracts.

Chips Inc., a semiconductor (SC) company used by the organization to produce military and aerospace systems, is considering a partnership with American Systems Co. to leverage their fabrication facility. This would represent a significant change in the supply chain related to a critical system element. American Systems Co. formed a task force in conjunction with Chips Inc., to help identify risks in the potential partnership and how they can be mitigated by both companies and their contractors.

10.2.2 Threat Source

American Systems Co. is concerned about the intellectual property and their patents regarding the Chips Inc. fabrication facility. They would like to monitor and control for chip over-production and mitigate loss of IP or extra chips that might end up in their competitor's hands. These critical capabilities are currently innovative and a key driver of American Systems Co.

Additionally, Chips Inc. is located in Hong Kong and in reviewing the financial viability of the company, American Systems Co found that they receive considerable government subsidies to encourage technical sector companies in Hong Kong.

10.2.3 Vulnerability

This is a risk with regard to insiders, as Chips Inc. has had a government subsidy and may lose that subsidy which keeps the company viable.

This may result in the sale of sensitive IP that belongs to American Systems Co.

Chips provides field service teams in 15 countries to service the chips and platforms manufactured by them. Within the United States (U.S.), the field services are provided by a contractor who outsources to subcontractors in various geographical locations to provide coverage in the U.S.

10.2.4 Threat Event Description

The contractors and subcontractors all wear the same TechServices polo shirts and name badges when they are performing onsite services. Through these support contracts, TechServices personnel are able to access American Systems Co.'s field sites across the country, including sensitive or critical facilities. The contractors

have access to spare parts at all times as some of the response times for customer outages have a 2 hour performance window.

10.2.5 Outcome

N/A

10.2.6 Organizational Units / Processes Affected

The risks of bringing aboard a new vendor is an important task and the challenge of working with a vendor that supports their products directly requires a more extensive vetting and monitoring.

This vendor onboarding process includes parts and components that involve sensitive American Systems Co. intellectual property. Chips Inc. has direct access to the electronic circuit design, testing and packaging aspects of American Service Co.'s intellectual property. They will have unique access to supply / demand data as they'll know how much product American Service Co.'s buys and where the company requests shipments to be delivered. Since Chips Inc. takes care of shipment and delivery of the products, they have exceptional knowledge of the processes that American Service Co.'s product use to receive, integrate and support the products they make.

Finally, Chips Inc. supports their customers' deployments of their fabricated chips and technologies by way of TechServices. TechServices is a value added service which maintains replacement parts and contains technicians on a 24/7 basis to respond to customer outages and issues very rapidly. While the parts are held separate from the technicians, Chips Inc. does provide the service and has extensive knowledge and access to American Service Co.'s sensitive operational facilities, internal processes and extensive access to spare parts, and lastly, since TechServices is contracted and subcontracted, other companies and personnel from higher risk personnel, may actually be the ones delivering services to your company, gaining access to critical facilities and having access to parts before they are installed into American Service Co.'s systems. There is likely no prohibition that TechServices can provide services to American Service Co.'s competition and may share data verbally or otherwise to their competition.

10.2.7 Potential Mitigating Strategies / SCRM Controls

A broad-based team focus and engagement strategy to work with Chips Inc. is essential to elicit all the potential risks and then develop risk mitigation strategies. Using the NIST SP 800-30 Rev. 1, and 800-171 or ISO IEC 27036 you can conduct risks assessments and perform risk management functions.

Potential Mitigating Strategies could include:

- Phasing of the onboarding of services. Initial services to fabricate chips should be developed first. Additional services provided by Chips Inc., such as TechServices can be phased in after initial risks and monitoring are in place;
- For delivery and distribution, American Service Co can keep its existing distribution center to receive deliveries and monitor parts from Chips Inc. for compliance. The common distribution center can effectively shield off much of American Service Co.'s infrastructure and operations from Chips Inc. insights;
- American Service Co can work with Chips Inc. procedures and work to update any lost or non-compliant chips and products;
- Limit American Service Co.'s, Point of Contacts (POCs) who interact with Chip Inc. from an acquisition standpoint. Make those POCs clear to Chips Inc. and give the POC's training to identify what data and types of data to share with Chips Inc.;
- Agree to security measures for transmission, encryption, storage, retention and destruction process and required paperwork of intellectual property shared to Chips Inc.;

- When American Service Co. decides to utilize support services from TechServices, American Service Co. can request TechServices employees have a background check before being allowed to participate on its contract. The same request can be done for Chips Inc. employees that interface with American Service Co.; and
- American Service Co should monitor the financial performance of Chips Inc. on a quarterly or bi-annual basis to monitor for changes in the company's financial performance or leadership changes.
- Flow-down security and risk-management policies to the supplier(s)
- Perform periodic audits of the supply chain.

10.3 SCENARIO: STAFFING FIRMS USED TO SOURCE HUMAN CAPITAL

10.3.1 Background

Nation state threat actors utilize a myriad of vectors to insert, influence, turn, or threaten company insiders into a compromising position, often resulting in the loss of a company's confidential or classified data or impact to a company's critical systems and services.

NIST defines an Insider as: One who will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the entity they work for. This threat can include damage through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of entity resources or capabilities.

While it is common for a nation state threat actor to apply leverage to an existing company insider in order to achieve a specific goal, the unwilling or untrained insider threat can often be more easily identified as compared to a planted insider. In any case, companies should have an operational Insider Threat Program (ITP) [NIST 800-53 & 800-171] wherein they employ active controls and awareness training to collect automated and manual notifications of potential insider threats.

In addition to the internal controls for the detection and prevention of insider threats, companies must also consider the insider threats stemming from their supply chain; in this scenario, the focus is the sourcing of employees, contractors, and consultants.

10.3.2 Threat Source

The threat source, in this example, is a nation state having influence over a staffing firm used by a company to source human capital. Staffing firms are often leveraged for two primarily purposes; (1) to source employee candidates, and (2) to provide skilled contractors or consultants as part of fixed-priced services.

In either case, the sourcing of candidates performed by the staffing firms can be manipulated to ensure certain qualified candidates (who are also insider threat agents) gain the first opportunities for employment. If selected for employment or contractor or consulting services, the threat agents begin to leverage access permissions to escalate privileges and acquire or disseminate data to unauthorized entities.

10.3.3 Vulnerability

The vulnerability in this example involves the partnership with a third party staffing firm who is instrumental in sourcing candidates for employment, and of which the staffing firm can be leveraged by a nation state to manipulate the recruitment and candidate sourcing to a company. In many of these cases, the staffing firm has offices around the world, while also having a recruitment or candidate database that can be accessed and modified by the staffing firm's international associates, with the intent of strategically planting insider agents into the recruitment process of a company.

Background checks can be effective for preventing the hiring of known malicious characters, but they may not detect willing insider threat agents. Also, if the staffing organization is offshore, background check policies,

procedures, and mechanisms may be inadequate to appropriately vet personnel. While it is important to maintain controls that detect and stop insider threat activity, preventing the hiring an insider threat agent can help mitigate this risk. This requires the adoption of SCRM controls to be applied to staffing firms. Hardware supporting their network routers, switches and hubs had not been upgraded in five years, which exposed the firm to a vulnerability, a shortcoming or hole in the security of an asset.

10.3.4 Threat Event Description

An insider threat agent successfully navigates the hiring process and secures employment (full-time, part-time, contractor, or consultant) with the target company. The insider agent uses their authorized access to acquire confidential or classified data and attempts to escalate their privileges when needed to acquire data when access is not currently granted. The insider agent maintains a slow and undetectable process for data exfiltration. This activity could last for years without detection. When finally detected years later, the investigation found that the agent was sourced from the company's staffing firm. Background checks at the time of hire did not find anything to highlight the potential threat.

10.3.5 Outcome

Nation state extracts technology and data that allows them to influence financial markets, reverse engineer product or services, and give a tactical or competitive advantage to its cause.

10.3.6 Organizational Units / Processes Affected

The affected organization is the organization that sources candidates from the staffing firm which is had an unknown international presence. The insider agent can affect the company's competitive edge, customer market percentage, reputation, and result in financial and regulatory penalties.

10.3.7 Potential Mitigating Strategies / SCRM Controls

The potential mitigating strategies would be an element of the risk management process as described by the Risk Management Framework. See the following for more information: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

Potential Mitigating Strategies could include:

- Performing SCRM assessment on all staffing firms used to source candidates for privileged access roles; the assessment should ensure the staffing firm does not have an international database which allows remote locations to influence the candidate hire dataset for a company; and
- Perform background checks on all workers, including employees, contractors, and consultants; background checks for resources who have privileged access should be performed with repetition. Verify that the background check is appropriately comprehensive and reliable.

11.0 Threat Category: Inherited Risk (Extended Supplier Chain)

11.1 SCENARIO: SUB-AGENCY FAILURE TO UPDATE EQUIPMENT

11.1.1 Background

A Sub-Agency hadn't upgraded their hardware supporting their network routers, switches and hubs for greater than five years. As a result, this agency was unable to receive software updates and therefore putting their agency at a substantial risk and vulnerable position.

11.1.2 Threat Source

These disruptions have taken place across state and local agencies, the private sector, and even at home with personal routers. Threats can come from international unfriendly countries, hackers, etc. Furthermore, the attack can come at any time with persistence and can occur frequently if the condition is not fixed.

11.1.3 Vulnerability

Because this was a sub-agency on the entire agency's network, all sub-agencies became vulnerable. The software from a supplier is not being maintained to its current version across sub-agencies, which has created a vulnerability.

11.1.4 Threat Event Description

This is a network category threat, as business heads and CFO's must be made aware that cutting budgets from network infrastructure is no longer an option. This is due in large part because of the size and scope of the risk posed to an organization's network infrastructure.

11.1.5 Outcome

The objective of the threat actor can be network disruption, data theft, intellectual property and financial threats.

11.1.6 Organizational Units / Processes Affected

N/A

11.1.7 Potential Mitigating Strategies / SCRM Controls

Require flow-down controls and risk management for all subs to pass to any of their subs. Then require audits or compliance reports and attestations.

11.2 SCENARIO: SUB-AGENCY FAILURE TO UPDATE ENTERPRISE SOFTWARE

11.2.1 Background

Enterprise software from a supplier is not being maintained to its current version across sub-agencies.

11.2.2 Threat Source

This threat is applicable across federal, state & local agencies as well as the private sector. The threats could occur anywhere within the supply chain i.e., OEMs, manufacturers, integrators, third parties, etc.

11.2.3 Vulnerability

Unpatched applications.

11.2.4 Threat Event Description

Software is the threat category. The sample threat mentioned above could be a threat to many agencies who does not maintain supported software thresholds (usually 2 previous versions). Non-updated operating systems are also a threat. Some organizations are still running vulnerable and unsupported versions that were deprecated years ago.

11.2.5 Outcome

Intellectual property, network, and disruption are all applicable. Several cities have already had their networks locked up and threat actors are demanding financial settlement to unlock their network and devices.

11.2.6 Organizational Units / Processes Affected

Depending on the software, it could impact the OEM, the reseller or the integrator. There could be cost implications, the integrity of the company may be questioned etc. Out of date software (no longer supported by the OEM or third parties) places unnecessary risk on the agency. Unsupported software places security vulnerability upon the business and the agency. The threat is applicable at any time and persistent within the infrastructure.

11.2.7 Potential Mitigating Strategies / SCRM Controls

Require supply chain organizations to keep their applications and operating systems up to data and patched within 72 hours of a new patch. Require attestations of compliance. Perform periodic audits.

11.3 SCENARIO: INHERITING RISK FROM NTH PARTY SUPPLIER

11.3.1 Background

During the development of components (software or hardware), sometimes exceptions are taken in test cases deemed *noncritical* to the operation of the subcomponent. These are not necessarily the wrong decisions in the testing process, but the failure is a result of not maintaining this information as the element flows up in the supply chain. This results in a lack of traceability as these elements are integrated into higher level components and eventually end products or systems. Furthermore, this can lead to cascading minor errors resulting in a vulnerability or IP license violation in the final product.

11.3.2 Threat Source

This threat is sourced from known and trusted suppliers. It is not intentionally targeting the end procuring agency, but it manifests at that level in the delivered system. This threat typically manifests as a one-time vulnerability in the form of a bug. It is not specific to only software or firmware, although that is more likely. This is an unintentional threat that results from inheriting acceptable risk decisions made by a supplier further down the chain from the end producer of the final product or service. The deeper into the supply chain is occurs, the more difficult it is to identify in advance.

11.3.3 Vulnerability

Unlike a typical threat actor sourced attack on the supply chain, the inherited risk from a lack of transparency can be very difficult to identify and mitigate in advance. It is an accidental vulnerability that is part of the normal system development life cycle and is a known vulnerability, possibly mitigated through proper internal controls. This information is traced within the SDLC of the sourcing supplier and typically provided in release notes to the procuring entity. The challenge is the compounding effect of numerous separate and distinct test exceptions as the complexity and scale of a system increases.

11.3.4 Threat Event Description

This is an inherited risk as a result of the extended supply chain that is an accepted part of the supplier SDLC. It is possible that the subcomponent, assembly, or software is used in a system for which it was not initially intended. The resulting environmental changes or integration with other pieces results in the threat manifesting into an impactful failure.

11.3.5 Outcome

N/A

11.3.6 Organizational Units / Processes Affected

The lack of traceability as these elements are integrated into higher level components and eventually end products or systems can lead to cascading minor errors resulting in a vulnerability or IP license violation in the final product. The objective is not to perpetuate a threat. It is the result of a common trade off in any engineering process concerning cost, schedule and quality.

11.3.7 Potential Mitigating Strategies / SCRM Controls

Good engineering process will ensure that these decisions are documented, and traceability is provided vertically up the supply chain.

11.4 SCENARIO: MID SUPPLY INSERTION OF COUNTERFEIT PARTS VIA SUPPLIER XYZ TO TRUSTED/VETTED VENDOR

11.4.1 Background

During the supply chain process, it is possible that a third party, or upstream supplier ("Supplier XYZ") providing components (software or hardware) to a trusted vendor within a chain has not been vetted to the same caliber as the trusted vendor itself. This can lead to the opportunity of a threat agent delivering, installing, and inserting counterfeit elements to the trusted vendor.

11.4.2 Threat Source

The threat may be sourced by a variety of stakeholders, including the following:

- Nation state actors;
- Cyber criminals;
- Extended stakeholders utilized via Supplier XYZ; and
- Unvetted stakeholders in the extended supply chain, etc.

11.4.3 Vulnerability

The inherited risk from Supplier XYZ can be difficult to detect because stakeholders within the extended supply chain may be hard to trace and enforce the same level of vetting scrutiny as a trusted vendor will be receiving. This vulnerability is the result of an extended supply chain with an unvetted or poorly vetted supplier that has been accepted by the stakeholders using it.

11.4.4 Threat Event Description

This inherited risk effects the transit and integrity of the trusted supply chain. Supplier XYZ can serve as an incognito vehicle for introduction of hostile elements that the vetted supplier may integrate within a product, or component that may be purchased by consumers. If Supplier XYZ had integrated counterfeit parts wittingly, they could have the ability to affect the reliability of the supply chain, products or exploit consumer data.

11.4.5 Outcome

If intentional, Supplier XYZ's objective may be to negatively impact integrity or availability of products and services provided by the upstream trusted vendor. A secondary objective could be damage to the reputation of

the trusted vendor. It is possible that Supplier XYZ's objective is not intentional damage but is the result of poor vendor risk management practices.

11.4.6 Organizational Units / Processes Affected

This threat affects hardware and software components within the supply chain. The threat described above, is an inherited risk due to the accepted trust of an extended supply chain member that has not been vetted and trusted by the end buyer. This can lead to insertion of counterfeit products, as well as tampering of a legitimate and integral supply chain.

11.4.7 Potential Mitigating Strategies / SCRM Controls

This threat will persist until Supplier XYZ is identified as the source of the counterfeit materials and removed.

12.0 Threat Category: Economic

12.1 SCENARIO: FINANCIAL STRENGTH OF THE SUPPLIER

12.1.1 Background

Each company is different in capability to respond to financial problems. This depends on a number of factors; including personnel, size, scope of the company, access to capital, and even geographic location. At any point in time, this capability can change.

12.1.2 Threat Source

There is significant overhead in maintaining a secure operational environment within a business enterprise. Some firms operating on razor thin margins, or startups struggling to make a profit will be tempted to cut corners or accept risks that can open up attack vectors to a threat.

12.1.3 Vulnerability

The vulnerability in the scenario was created by not spending funds on using protective software.

12.1.4 Threat Event Description

A company struggling to survive under heavy financial stress just to meet payroll may cut IT staff, stop using protective software, or even share protected files or data with an unauthorized buyer just to stay afloat.

12.1.5 Outcome

These potentially bad results are predicated on weakness in financial strengths of a supplier. Unpredictable or surge orders or customers shifting to a new supplier can cause a company to rebalance to match income with expenses.

12.1.6 Organizational Units / Processes Affected

N/A

12.1.7 Potential Mitigating Strategies / SCRM Controls

Understanding the financial position of your suppliers can help deciding on the need for changes, mitigation strategies, or discussions on how you can help or advise suppliers on improving their operations. Reviewing financial reports from public companies, looking at reports from organizations like Dun & Bradstreet, or having

a one on one personal discussions and reviews can all help. A close personal relationship with suppliers will also help mitigate risk.

12.2 SCENARIO: INFORMATION ASYMMETRIES

12.2.1 Background

There will always be a difference between what the supplier knows and what the customer knows. Even for customers, who have people collocated with suppliers, this difference of insights or information can cause decision making that will open up potential threat vectors.

12.2.2 Threat Source

The problem from different knowledge or understanding of a supplier's financial status or economic conditions in the marketplace can create assumptions that everything is going fine, when in fact they aren't.

12.2.3 Vulnerability

Lack of oversight from the customer's perspective - built into contracts with the supplier.

12.2.4 Threat Event Description

The supplier is not following the processes or procedures in securing the product from either physical compromise or digital security of the design. The customer is not aware of their lack of compliance.

12.2.5 Outcome

The lack of information or the partial gathering of information can cause problems from the customer making assumptions that things are proceeding on plan and with approved and documented processes, but when the supplier knows that these efforts are not being maintained.

12.2.6 Organizational Units / Processes Affected

N/A

12.2.7 Potential Mitigating Strategies / SCRM Controls

Place people at the site of a suppliers' production or assembly to monitor or validate. This will incur additional costs but is a control step that reduces or mitigates risk in supply chin compromise.

12.3 SCENARIO: OWNERSHIP CHANGE

12.3.1 Background

Ownership of a supplier can change hands at any time. New investors will be brought into a small business or start up. Successful businesses will be acquired or merged with larger or equal size businesses. If the ownership change involves foreign entities, this can be problematic to the information security of the company.

12.3.2 Threat Source

Large amounts of cash generated by a successful business requires reinvestment. Letting cash sit around unproductively is not usually a smart way to grow a company. Often cash accumulation is used to acquire companies in vertical or horizontal markets.

12.3.3 Vulnerability

Lack of oversight from the customer's perspective - built into contracts with the supplier.

12.3.4 Threat Event Description

A large Chinese firm has successful been a supplier to numerous companies across the globe. This firm targets a U.S. firm in the same market that is considered a competitor for acquisition. This allows for horizontal integration at the same time as a reduction in global competition.

12.3.5 Outcome

The acquisition of firms that control a majority of the market can be considered an anti-trust violation in many countries. This concept or legal restriction does not apply worldwide. Firms that are controlled, subsidized or financially supported by governments can have an unfair advantage in the marketplace.

12.3.6 Organizational Units / Processes Affected

N/A

12.3.7 Potential Mitigating Strategies / SCRM Controls

The U.S. government should protect U.S. firms undergoing unfair competition. CFIUS should restrict sales of U.S. firms to foreign firms, where the acquisition would create a risk to the supply chain or a transfer of control of a critical market to oversight by a hostile of unfriendly government.

12.4 SCENARIO: COST VOLATILITY

12.4.1 Background

Outside of the suppliers' control, there can be governmental or economic drivers that will affect the cost of a specific product. While minor price increases or drops are usually accounted for in the markup of products at each stage of the supply chain, successful companies still have challenges when monetary policy (value of the local currency) is less than stable or when market related events occur (i.e. tariffs are employed for political purposes or economic downturn causes businesses to react differently). This can be quite problematic for multiple parts of the supply chain. This is especially true for ICT supply chain which works on thin margins to start with.

12.4.2 Threat Source

The value of currency and politically volatile events can have serious implications on taxes (tariffs) and the true cost of trade across multiple currencies. One way around this is to diversify your supply chain sources to develop contingencies should volatility arise on supply costs. This is part of a good supply chain risk management strategy.

12.4.3 Vulnerability

N/A

12.4.4 Threat Event Description

The Chinese government is suspected of limiting output of the rare earth element, neodymium, to a number of external suppliers. Neodymium is essential in the manufacturing of permanent magnets. Various countries have various amounts of Neodymium stockpiled for multiple industries. Neodymium has fluctuated extensively in price over the past 5 years and affects the pricing of hard drives and other electronics that much of the

world counts on from Vietnam, China and other Asian countries. Since China has over 90 percent of the earth's known quantity of Neodymium, at various times, they have taken political actions that cause dramatic volatility in the price and amount of Neodymium available worldwide.

12.4.5 Outcome

The ability for U.S. or other countries' to invest in Chinese mines has been very limited to non-existent by the Chinese government. Chinese firms have sought to invest in the companies that use the rare earths to expand their ability to control more of the technology marketplace. These firms are backed by the Chinese government and they're usually state owned or managed companies. They can use rare earths to affect prices outside the country (initiate volatility) and ensure supply and low cost for state owned companies (inside China) to affect the volatility, price and supply chains for various products.

12.4.6 Organizational Units / Processes Affected

N/A

12.4.7 Potential Mitigating Strategies / SCRM Controls

U.S. companies need to work with businesses and countries outside of China to diversify their supply chains and lower supply chain risks. R&D needs to consider possible replacements for rare earths that are politicized. Supply chains can, likely at additional cost, work to obtain and seek out rare earths from other sources. Additionally, some rare earths can be obtained at a lower price if they are provided before they're separated but will incur some cost for the separation of the rare earths from their source. The goal from these mitigations will likely yield a diversified source of products that can obtained needed Neodymium at a more stable price structure than competitors. Competitors will likely have to add margin to deal with the multiple variables that will add excess market costs to their supply chain.

13.0 Threat Category: Legal

13.1 SCENARIO: LAWS THAT HARM OR UNDERMINE AMERICAN ECONOMIC INTERESTS

13.1.1 Background

Under U.S. federal and (most) state law, trade secrets have protected status, which helps to enable the cyber supply chain to flourish. This same type of legal protections does not exist in every country where a company – or entities in the company's supply chain - is located or transacts business.

"China has implemented laws, policies, and practices and has taken actions related to intellectual property, innovation, and technology that may encourage or require the transfer of American technology and intellectual property to enterprises in China or that may otherwise negatively affect American economic interests. These laws, policies, practices, and actions may inhibit United States exports, deprive United States citizens of fair remuneration for their innovations, divert American jobs to workers in China, contribute to our trade deficit with China, and otherwise undermine American manufacturing, services, and innovation." Excerpt from Presidential Memo to the U.S. Trade Representative, 2017.

13.1.2 Threat Source

State and quasi-state threat actors refers to hostile governments that want to disrupt American cyber supply chains for strategic or tactical advantage. It is also a reference to any governing authority that de facto acts as a state. Lack of diplomatic recognition as a state does not affect the actor's ability to operate as a supply chain threat. These actors are defined by their strategic or tactical reasons for wanting to disrupt American cyber supply chains and their ability to employ state or state-like powers to achieve that end, not the formalities of diplomacy, such as state-owned enterprises—who would look to steal American intellectual property. State-

owned enterprises and similar quasi-state actors around the world seek advantage in the marketplace and in the operation of whatever end they are tasked by their associated government.

Quasi-state actors are largely synonymous with state-owned enterprises. These are businesses or organizations that operate independently of any government, at least on paper, but are influenced by a government to such a degree that the organization is either effectively owned or controlled by it. These quasi-state actors are different from state actors in that they have some private function—usually a market function—but nor can they escape government-given public functions. These public functions may include manufacturing of military equipment, maximizing employment, or dominating a sector seen as strategic to the state-actor's national interests.

13.1.3 Vulnerability

Businesses operating in or desiring to sell their goods to nation states, such as China, may be subject to legal requirements that could result in the loss of their intellectual property or the undermining of their market share.

13.1.4 Threat Event Description

The state actor opts against enforcing (or not having) intellectual property protections and forces technology transfers. This allows a state actor to unleash non-state third parties and quasi-state actors to pursue their objectives to steal intellectual property without domestic legal consequence. A more overt method of obtaining IP is via forced technology transfers (a government-mandated transfer of intellectual property from the original owner to some other entity).

13.1.5 Outcome

This fundamentally harms trade secret protections. Further, once stolen intellectual property is in the wild and with few legal protections and remedies, it can result in counterfeit parts and sabotage that may cause disruptions in the cyber supply chain, denial of end products, and failure of the end products.

13.1.6 Organizational Units / Processes Affected

N/A

13.1.7 Potential Mitigating Strategies / SCRM Controls

There are limited mitigation options. Suppliers should be aware of the legal requirements of the countries in which they operate, do business and consumers should be aware of which of their suppliers may be subject to these onerous laws.

13.2 SCENARIO: LEGAL JURISDICTION-RELATED THREATS

13.2.1 Background

Company A relies upon a foreign-based manufacturer to produce a key component of its product. The country the manufacturer is located is known for government corruption and weak oversight of its domestic businesses

13.2.2 Threat Source

Supply chain entity is threat actor: Entities within the global supply chain can intentionally or unintentionally introduce threats into an end product deliverable. Actors may have nefarious intent, be profit-motivated, or simply negligent.

13.2.3 Vulnerability

A threat actor has the opportunity to engage in nefarious behavior in a jurisdiction unlikely to punish or deter such behavior. The problem of security become more complex and therefore more expensive.

13.2.4 Threat Event Description

The manufacturer uses inferior material to produce the components for Company A while charging Company A for the costs of the more expensive, specified material and falsifying its financial records. Manufacturing company managers pocket the savings in costs they generate from using cheaper material. This introduces a weakness in the product that cannot be readily identified but will cause the component and to fail prematurely.

13.2.5 Outcome

Poor security from entities within a supply chain has potentially devastating implications for delivery of an end product. When the supply extends across multiple countries, differing legal jurisdictions introduce multiplied and varied threat opportunities.

13.2.6 Organizational Units / Processes Affected

N/A

13.2.7 Potential Mitigating Strategies / SCRM Controls

Businesses offering goods and services should carefully vet the businesses within their own supply chains to ensure that the deliverables they provide to their customers will appropriately perform and be trustworthy. In this scenario, Company A may want to consider controls such as third party auditing or monitoring, oversight of manufacturing processing by on-site Company A personnel, or a product testing program to ensure the components delivered are conformant to specifications. Acquirers' of Company A's products should seek to understand how Company A ensures the quality and trustworthiness of its products- especially if the product is intended to be used for a critical mission or business purpose.

13.3 SCENARIO: LEGAL COSTS THAT WEAKEN THE FINANCIAL VIABILITY OF A COMPANY

13.3.1 Background

A medium sized business provides a niche service to a Government customer that is critical to the Government customer's mission. There are only a handful of other businesses in the marketplace that can provide this service.

13.3.2 Threat Source

N/A

13.3.3 Vulnerability

The medium sized business has limited cash reserves and has made a business decision to reinvest a majority of its profits to grow the business through marketing and an expansion of its sales force. While the business has made some investments in new technology and has a small team that manages the IT, there are no dedicated personnel focused on IT security and only basic security protections are in place.

13.3.4 Threat Event Description

One of the IT personnel finds evidence that one of the systems may have been breached. This system contains employee related data that is confidential in nature. After hiring a security firm, the evidence was insufficient to

be able to determine whether a breach actually occurred and if so, whether data were accessed. The business' legal firm advises that all company personnel must be notified and offered identify protection services for no less than one year. The business is also advised that they must notify their government customer, per their contract terms and conditions. The company fears their contract may not be renewed. Legal costs are significant.

13.3.5 Outcome

According to a study at Champlain College, sixty percent of Small and Medium-sized Businesses (SMBs) will go out of business within six months after a data breach. The reasons for this are not likely to be exclusively legal, but the legal costs associated with a data breach are certainly significant for SMB suppliers in the cyber supply chain and there is the potential for resultant business closures.

13.3.6 Organizational Units / Processes Affected

N/A

13.3.7 Potential Mitigating Strategies / SCRM Controls

It is important to consider to what extent unplanned for legal costs may undermine the financial viability of a small or medium sized company. If this business provides a critical service or product, it would be prudent to investigate the strength of the company's financial resources prior to engaging in a contractual relationship or ensure that there are readily available alternative sources of supply that could be quickly acquired should the firm find itself in unanticipated financial trouble and go out of business or fail to perform satisfactorily due to constrained resources.

This scenario describes legal costs that arise out of a data breach. Other sources of legal costs can include: settlements and pending litigation against a business, fines and penalties levied against the company, and contractual-related liabilities arising from actions such a termination for cause or stemming from threats introduced by extended supply chain partners or sub-tier subcontractors.

14.0 Threat Category: External End-to-End Supply Chain

14.1 SCENARIO: NATURAL DISASTERS CAUSING SUPPLY CHAIN DISRUPTIONS

14.1.1 Background

External events including natural disasters can have a large impact on the end to end supply chain ranging from destruction of manufacturing facilities, the ability to receive production materials to the ability of workers to get to work, to the ability to distribute final products to mention only a few. Depending on the size and scope of the event, the disruption to the end-to-end supply chain can have multiple impacts.

14.1.2 Threat Source

Natural disasters can have a severe impact on our global economy. According to Aon Benfield's 2016 Global Climate Catastrophe Report, the world saw $210 billion in economic losses because of 315 separate natural disasters. That's 21 percent above the 16-year average of $174 billion. In 2017, Hurricane Harvey victims saw over 178,000 homes lost, $669 million in damages of public property, around a quarter million vehicle losses, $200 million in Texas crop in livestock losses. Additionally, businesses saw significant and expensive losses due to flooding, electrical outage, and employees' inability to get to work, all causing temporary disruption of the flow of goods and services. But the impacts of natural disasters reach far beyond the local damages of affected areas. When these natural events happen, many businesses find their supply chains greatly impacted.

The Tohoku Earthquake and Tsunami in Japan and the Thailand Floods in 2011 are both examples of natural disasters that had expanded indirect economic effect. Both disasters caused severe disruption to global

technology supply chains. After the Thai floods, there was a global shortage of computer hard drives that sent consumer prices skyrocketing until factories were able to get back up and running. When the 2011 tsunami struck, several major until business operations were restored to normal. Car manufacturers were forced to shut down production at factories throughout Europe and the U.S. due to a lack of available parts from factories in Japan, setting off a supply chain reaction that impacted multiple suppliers of parts throughout the wider global economy.

14.1.3 Vulnerability

N/A

14.1.4 Threat Event Description

A category 5 hurricane has hit in Savanah, GA, and has moved up the east coast and inland in northern VA before becoming a tropical storm. The hurricane damaged or destroyed ports from Savanah, GA to Norfolk VA while also destroying roads and bridges. Critical infrastructure impacts were also wide spread, specifically impacts to power and communications.

14.1.5 Outcome

The ever-growing reach of global supply chains exposes these networks to serious vulnerabilities. In this scenario, a medium sized manufacturing company has been impacted in several ways. First there are impacts to getting materials into the manufacturing plant and the ability to distribute and finished products leading to financial harm, such as unrecoverable loss of revenue or accounts receivable, as well as contractual fines and penalties; the inability to provide effective customer relations and regulatory reporting; and damage to relationships, brand or corporate reputation and confidence.

14.1.6 Organizational Units / Processes Affected

N/A

14.1.7 Potential Mitigating Strategies / SCRM Controls

Following established steps to identify potential risks to the supply chain and plan for business interruptions is critical for a company's survival in times of natural disasters.

The first step is to complete a Business Impact Analysis (BIA). This analysis provides a complete understanding of the business and its supply chain, allowing organizations to identify exposures and potential mitigation measures. It helps identify the most feasible and cost-effective strategies and solutions for business continuity and disaster recovery. In addition, reviewing insurance policies as they relate to business interruption enables companies to detect any areas requiring additional coverage.

Following the BIA, the second step is disaster recovery preparation. Based on the results of the impact analysis, this exercise finds critical business functions, resources and methods; reveals business unit, supplier and customer interdependencies; further identifies potential threats and exposures; and helps users ascertain potential losses and impacts, should a disaster occur. The process involves documenting recovery time objectives, IT interdependencies and manual procedures; evaluating existing recovery capabilities; and creating effective mitigation measures, including the recovery plan documenting who to call, where to go and who will do what in the event of a disaster. It also identifies which tasks must be considered mission-critical. The plan sets a schedule for periodic backups of all electronic and hard-copy documentation, which should be stored in an alternate location.

Focus on creating a stable, yet flexible, supply chain. Diversifying suppliers and methods of transport wherever possible is an effective strategy. Also consider alternate supplier teams and define roles both internally and

externally to enable this emergency supply chain. Backup work locations, redundant IT systems should also be a priority.

The body of the recovery plan should include the following:

- Business assumptions;
- Incident-management team member including critical personnel from all areas of the company resources and recovery assignments;
- Recovery strategy and solution overview;
- Emergency-response procedures;
- Incident-reporting procedures;
- Recovery team notification, mobilization and assembly procedures;
- Detailed recovery procedures;
- Situation-assessment guidelines;
- Emergency contact information of key employees, vendors and customers;
- A summary of mission-critical business functions to be recovered; and
- Detailed procedures for transitioning back to business as usual.

Finally, the third step in the process is to regularly test the plan. A plan is only as good as its execution. A table top exercise is an effective way to test and validate the plan by ensuring all internal and external team members are familiar with their roles and responsibilities. Aside from assisting team members practice their roles, develop confidence and expertise it can reveal any necessary gaps and needed updates.

14.2 SCENARIO: MAN MADE DISRUPTIONS: SABOTAGE, TERRORISM, CRIME, AND WAR

14.2.1 Background

Man-made events such as fire, product defects, cyber-attacks, labor and civil unrest, terrorism, utility failure, and piracy are frequent disruptors of supply chains, but typically have a lower severity than natural catastrophes.

14.2.2 Threat Source

The year 2016 saw several man-made disruptions, including the late summer Gap warehouse fire in Fishkill, New York, which destroyed 30 percent of Gap's total warehouse space and disrupted more than 10 percent of Gap's orders. Another example is the Samsung Note cellphone battery recall, which was linked to problems in a battery supplier's supply chain and had far-reaching consequences for the Samsung brand and their customers.

The past few years have seen an increasing prevalence of cyber-attacks. Most of these incidents, such as the high-profile Equifax data breach that involved the personal information of some 143 million Americans, and the Dyn cyber-attack which took down some of the world's most popular websites such as Twitter, Airbnb, and Netflix, do not directly affect supply chains. However, they raise major red flags for supply chain practitioners. It seems that cyber criminals have a growing number of avenues of attack at their disposal, especially given the exponential growth in the number of Internet-enabled devices and cloud-based communications networks.

14.2.3 Vulnerability

N/A

14.2.4 Threat Event Description

The collision of carriers in the waterway ceased operations at the Twin Ports. The collision resulted in one of the vessels taking on water, which caused the vessel to capsize dropping the containerized units from the vessel into the waterway, destroying the products in the containerized units

The cargo carriers not affected in the collision sat idle until which time they received direction from the port authorities on how to proceed. The carriers were either directed up the coast to a different port or were instructed to stay put until they could resume operations and accept the cargo at the Twin Ports.

14.2.5 Outcome

The majority of overseas cargo comes from Asia and therefore come into ports on the West Coast. Los Angeles and Long Beach handle over 40 percent of U.S imports from Asia. Due to the heavy cargo traffic, a collision of 2 cargo ships occurred in the waterways halting operations to the Twin Ports in Los Angeles and Long Beach.

14.2.6 Organizational Units / Processes Affected

The collision created a delay in delivery of network components to the U.S. Company. The components could have been destroyed if they were in a containerized unit that fell into the water, or a significant delay could occur if the components were on a ship that was re-routed to a different port due to the port closures at Twin Ports.

The U.S. Company was able to track down their shipment and determined that it was taken to a port in New Jersey and arranged for ground transportation to obtain the shipment and deliver to the U.S. Company.

The U.S. Company missed their committed lead times resulting in a delay in delivering their network equipment to customers. Due to the missed due dates, the U.S. Company was expected to pay liquidated damages that were contractually agreed to with their customers.

14.2.7 Potential Mitigating Strategies / SCRM Controls

To avoid future scenarios such as the one described above, the ports should monitor the traffic 24/7 to avoid congestion of ships when approaching the ports.

Additionally, a protocol should exist amongst ships that if any ship is within .5 miles from another ship, the ships communicate with one another and, based on the protocol, one ship remain idle until the other ship has cleared the port.

14.3 SCENARIO: LABOR ISSUES

14.3.1 Background

An organization has decided to perform a threat scenario analysis of its resource and capacity planning. The scenario will focus on the sensitivity of the business to unforeseen fluctuations in the country's unemployment rate.

14.3.2 Threat Source

GoFast Auto Company is a 1.5 million square foot manufacturing facility that produces 45 million automotive parts per year. The company supplies mainly to after-market retailers but does have some direct contracts with major automotive manufacturers in the United States to produce proprietary parts. There are 35,000 employees, 28,000 of which are directly tied to production and run three full shifts. The production organization is made up of machinists, technicians, inventory control, quality assurance, design engineering, and other occupations ranging in skill and education level.

14.3.3 Vulnerability

N/A

14.3.4 Threat Event Description

The organization has established the following fictitious threat for the analysis exercise:

Two years ago, there had been a lot of political momentum to enable better, higher-paying jobs in manufacturing and other blue-collar jobs. Due to this, a year ago, there were several programs that were funded by the U.S. government to encourage brining jobs back to the U.S. from oversees locations while also increasing wages. After three phases of these programs touching on different industries, the U.S. has seen its unemployment rate drop from 8.5 percent to 3.4 percent.

14.3.5 Outcome

With unemployment at low levels, there has been a lot of job movement, particularly in the manufacturing sector. As a result of this, GoFast has seen attrition at 3x the normal rate. Labor levels have dropped off to the point where the production of some components has had to be delayed or even halted. The reduction in volume produced has directly led to a drop in revenue, and one contract for proprietary parts was terminated. In 6 months, revenues have dropped 13 percent.

GoFast attempted to rectify some of the impact by moving employees into more critical roles, but generally, the training time for a major role change is approximately 4 months. Additionally, GoFast has reached out to several consulting and staffing firms, but there are two issues with this. One is the personnel from these outlets would take even longer (6-8 months) to fully ramp up as they are brand new to the company, and two is even the staffing firms are having trouble attracting skilled talent.

14.3.6 Organizational Units / Processes Affected

N/A

14.3.7 Potential Mitigating Strategies / SCRM Controls

- Institute a standard rotation or cross-training process for all, or at least employees in critical roles;
- Offer more competitive packages for skilled people looking for new opportunities in the marketplace;
- Entice more employees to stay with perks, including wage increases, benefits, time off, educational and training opportunities, flexible hours, or other options that make sense for employee and employer;
- Simplify processes or improve related training and documentation to reduce transition or onboarding time for folks new to an area; and
- Work with local trade schools and universities to develop talent with specific skills that are currently lacking in the workforce.

14.4 SCENARIO: INFLUENCE OR CONTROL BY FOREIGN GOVERNMENTS OVER SUPPLIERS

14.4.1 Background

An organization has decided to perform a threat scenario analysis of its Printed Circuit Board (PCB) suppliers. The scenario will focus on the sensitivity of the business to unforeseen fluctuations in component costs.

14.4.2 Threat Source

Apex PC Corporation designs, assembles, and ships 3.5 million personal computers per year. It has a global footprint both in terms of customer and supply bases. Five years ago, in an effort to reduce the cost of goods sold, Apex shifted a majority of its PCB procurement to Southeast Asia. In an effort to not be single sourced, Apex finalized agreements with five different suppliers within the country and has enjoyed a positive partnership with each during this time.

14.4.3 Vulnerability

N/A

14.4.4 Threat Event Description

The organization has established the following fictitious threat for the analysis exercise:

Last year, the country where Apex does most of their PCB business has seen a new regime take over the government. This regime has been more focused on improving finances and business environment within the country, allowing larger firms who set up headquarters and other major centers within country advantages to more easily and cost-efficiently do business with suppliers within the same region.

In February of 2019, this now-corrupt regime has passed new legislation that establishes an additional 20 percent tax on all electronic components and goods sold outside of the country. This new law was to take effect on June 1, 2019.

At the time the new law was announced, the current Apex inventory of PCBs was about 10 percent of yearly demand, which was the typical level of inventory they were comfortable with. Before June, Apex reached out to all five suppliers to order additional materials, but there was quickly a shortage due to higher demand from many foreign customers of these products. By June 1, the day the new tax law took effect, Apex was up to an inventory level of up to 15 percent of yearly demand.

14.4.5 Outcome

Between February and June, Apex also looked to partner with new suppliers, but there were several issues found with this. For one, of the 10 new suppliers Apex reached out to, the lead time for ramping up to desired demand was anywhere from 6 months to 18 months. This would include work on Apex's end, to include testing samples of the supplier PCBs and working out logistics details, to supplier-side activities such as procurement of raw materials and acquisition of additional personnel, production space, etc. necessary to meet the new demand.

The second issue is due to the current contracts with all five current suppliers in Southeast Asia, there were minimum demand requirements, meaning Apex was committed to purchasing a minimum of 100,000 PCB's per month for the duration of the contracts (which ranged anywhere from 3 months to 24 months remaining). This would mean Apex could not easily avoid the cost implications of this new tax.

Could Apex absorb the cost of the PCBs? With a 20 percent cost increase, this eroded the margins of a PC from 13.5 percent down to 4.5 percent, on average. For some of the lower margin Apex offerings, it would likely mean discontinuing the line and using these now more expensive PCB's on higher-end models that could carry more margin.

14.4.6 Organizational Units / Processes Affected

N/A

14.4.7 Potential Mitigating Strategies / SCRM Controls

- Diversify suppliers not just by immediate location, but country, region and other factors;
- Build cost implications into supplier contracts, making it easier to walk away from suppliers when costs rise too high (whether its fault of the supplier or not);
- Adjust desired inventory levels to better account for unexpected shortage of demand at critical times; and
- Employ more resources in countries or regions of key suppliers in hopes of receiving advanced Intel of new legislature that may negatively affect business.

14.5 SCENARIO: MALICIOUS SUPPLIER INSERTS HOSTILE CONTENT

14.5.1 Background

A software supplier, NMT-Com provides network management infrastructure for numerous global companies. Recently, several customers have complained about products that have ended up failing certain security scans upon receipt, although the majority of customers have had no reported issues.

14.5.2 Threat Source

NMT-Com has software developers around the world, with a dozen different code compiler locations, at their primary development centers. Software packages and libraries are uploaded for review and security scanning and then stored where they can be utilized by developers within the region; customer support is handled by the regional center that supplies the software load.

Product packages are intended to be consistent across customers, for easier support, patching and development. Release testing is done on a periodic basis in the development cycle at each center.

14.5.3 Vulnerability

According to the scenario presented, since NMT-Com has a dozen difference code compiler locations, there is the potential for a bug to be inserted into the code, thus creating a vulnerability.

14.5.4 Threat Event Description

A malicious supplier employee inserts hostile content at the product or component manufacturing or software compilation stage to affect supplier products or components delivered to a targeted subset of downstream customers.

14.5.5 Outcome

Due to the disconnect between the process of where software is scanned and where it is compiled and released, there is a potential for insertion of malicious software. There is an assumption of trust at the compiler locations and no re-scanning is done, except on the full release on a periodic basis (rather than every time it is changed and before it is signed.

This could leave customers of the supplier open to backdoor exploits, software injection attacks, data manipulation, data exfiltration or any number of attacks possible if the very code itself is compromised.

14.5.6 Organizational Units / Processes Affected

N/A

14.5.7 Potential Mitigating Strategies / SCRM Controls

- The supplier should implement, monitor and audit a comprehensive security assurance framework as part of their software development process;
- All software should be compiled in trusted locations, such as where it is also verified, scanned and signed. This would also serve as a logical central distribution point. Whenever software is changed and re-compiled, there could be a potential for injection of malicious code; thus, security scanning should be performed on each of these loads; and
- Static and dynamic code inspection is commonly used to verify the security and integrity of software. Static testing involves checking the code from an internal standpoint, executing code paths and routines to ensure they are operating as expected. Dynamic (aka black box) testing involves mimicking attacker behavior from the outside, detecting known vulnerabilities and simulating theoretical ones to determine if the product is vulnerable to different kinds of exploits.
- Consider keeping code repositories and compiling functions in the cloud.

DHS POINT OF CONTACT

National Risk Management Center
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
NRMC@hq.dhs.gov
For more information about NRMC, visit www.cisa.gov/national-risk-management

PDM20003

Appendix 2

CISA 5G RDT&E Efforts Infographic, CISA, May 2020

CISA 5G Research, Development Testing, and Evaluation (RDT&E) Efforts

In alignment to the *National Strategy to Secure 5G* and the *Cybersecurity and Infrastructure Security Agency's (CISA) 5G Strategy*, CISA will conduct RDT&E to help ensure interoperable, secure, and resilient 5G capabilities across National Critical Functions (NCFs) and National Essential Functions (NEFs). The following chart illustrates three major components of the 5G Network and describes CISA's current RDT&E Objectives and Focus Areas for each component.

USE CASES

Mobile End User Devices

Internet of Things (IoT)

Objective:

Secure end user equipment and protect personal data, information, and confidentiality.

Focus Areas:

CSD: User Device Operating Systems, Data Integrity, Systems Security, Access Control, Confidentiality (encryption)

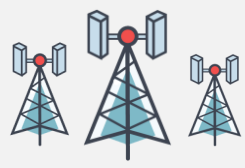
ECD: Massive IoT, Data Management

IOD: Secure voice and text applications (apps), Sensitive But Unclassified (SBU) Apps and Conferencing

NRMC: IoT, Machine to Machine (M2M)

RADIO ACCESS NETWORK (RAN)

Small Cells



Macro Towers

Baseband Unit (BBU) Pool

Objective:

Mitigate legacy vulnerabilities and enhance the security of 5G infrastructure components to ensure continuity of service.

Focus Areas:

CSD: gNodeB Functionality and Security Analysis (5G NR Base Station)

ECD: Edge Computing and Security

NRMC: Interoperability initiatives like Open Radio Access Network (O-RAN), Threat Detection and Protection of Current and Legacy Protocols, Open Air Interface (OAI) Software, Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD) testing on 5G Infrastructure

CORE NETWORK

Core Network Infrastructure

Objective:

Prevent unauthorized access to backend systems and degradation or denial of service through virtual infrastructure.

Focus Areas:

ECD: Virtualized Core Networks

NRMC: Cloud-Native 5G Core

CROSS-CUTTING FOCUS AREAS

Cybersecurity Division (CSD):
Data Integrity, Denial-of-service (DoS)/hacking

Emergency Communications Division (ECD):
Identity, Credential, and Access Management (ICAM), Priority Services, Network Function Virtualization (NFV), Software Defined Networking (SDN), Network Slicing

Integrated Operations Division (IOD):
Intrusion Detection and Prevention Systems (IDPS)

National Risk Management Center (NRMC):
SDN, End-to-End (E2E) Encryption and Security Solutions for Devices and Networks

BAA SOLICITATION

The Broad Agency Announcement (BAA) solicitation, published in April of 2019 between CISA and the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), is a tool that gives CISA the ability to solicit and efficiently execute research and development efforts with business, industry, and academia. Through this acquisition mechanism, CISA is also able to effectively coordinate and deliver 5G RDT&E solutions and programs with other federal departments and agencies.

FEDERAL PARTNERS

Homeland Security
Science and Technology

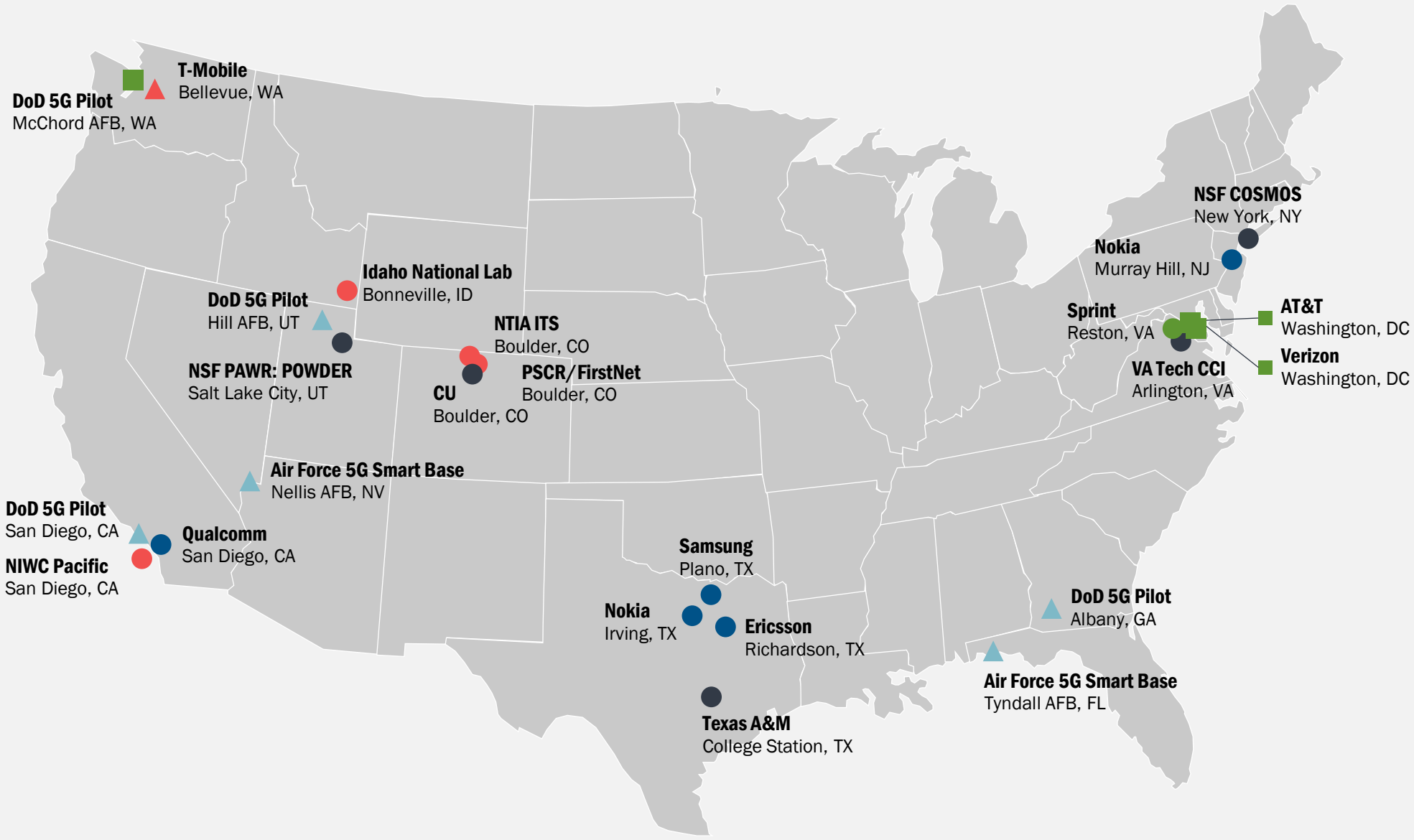
NIST
National Institute of Standards and Technology

Nationwide 5G Labs and Testbeds

Lab/Testbed Visit Observations

DHS visited and assessed a series of labs and testbeds to enhance interagency collaboration, inform federal agencies about capabilities and testing approaches, and provide a common understanding of 5G for agency leaders. The labs and testbeds surveyed consisted of those built with carrier grade equipment, federal labs, and academic institutions. The following is a summary of DHS's findings:

- Equipment manufacturer labs are a viable option for federal government testing needs. Their equipment conforms to 3rd Generation Partnership Project (3GPP) standards and continues to evolve.
- Labs operated by cellular carriers focus on testing features and interoperability prior to deployment of services. As a result, it is unlikely that cellular carriers would be able to provide lab services for the government. However, agencies do need to work with carriers to temporarily gain access to spectrum for testing purposes.
- Federal labs are an ideal option for conducting open-field, outdoor scenarios and testing specific requirements that present a straightforward approach for federal agency use.
- University labs and testbeds are an option for conceptualization, mid-to-long-term research and development, and campus testing.



Map Key:

- ○ 4G/5G Lab Visits Completed
- △ To Be Determined Lab Visits
- □ Virtual 5G Discussions
- ● ▲ Carrier Grade Equipment: Original Equipment Manufacturer (OEM)
- ● ■ Carrier Grade Equipment: Cellular Carriers
- ● ▲ DoD Pilot Sites
- ● ▲ Federal 5G Labs
- ● ▲ University 5G Testbeds

Appendix 3

Overview Of Risks Introduced By 5G Adoption In The United States, CISA, July 31, 2019

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE NOTE

July 31, 2019; 1200 EDT

OVERVIEW OF RISKS INTRODUCED BY 5G ADOPTION IN THE UNITED STATES

KEY FINDINGS

The Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) assesses that Fifth Generation Mobile Network (5G) will present opportunities and challenges, and its implementation will introduce vulnerabilities related to supply chains, deployment, network security, and the loss of competition and trusted options.

- Use of 5G components manufactured by untrusted companies could expose U.S. entities to risks introduced by malicious software and hardware, counterfeit components, and component flaws caused by poor manufacturing processes and maintenance procedures. 5G hardware, software, and services provided by untrusted entities could increase the risk of compromise to the confidentiality, integrity, and availability of network assets. Even if U.S. networks are secure, U.S. data that travels overseas through untrusted telecommunication networks[i] is potentially at risk of interception, manipulation, disruption, and destruction.
- 5G will use more components than previous generations of wireless networks, and the proliferation of 5G infrastructure may provide malicious actors more attack vectors. The effectiveness of 5G's security enhancements will in part depend on proper implementation and configuration.
- Despite security enhancement over previous generations, it is unknown what new vulnerabilities may be discovered in 5G networks. Further, 5G builds upon previous generations of wireless networks and will initially be integrated into 4G Long-Term Evolution (LTE) networks that contain some legacy vulnerabilities.
- Untrusted companies may be less likely to participate in interoperability efforts. Custom 5G technologies that do not meet interoperability standards may be difficult to update, repair, and replace. This potentially increases the lifecycle cost of the product and delays 5G deployment if the equipment requires replacement. The lack of interoperability may also have negative impacts on the competitive market as companies could be driven out if the available competitive market decreases.

The United States Government can manage these vulnerabilities and increase the security of communications networks as 5G is adopted by:

- Encouraging continued development of trusted 5G technologies, services, and products.
- Encouraging continued trusted development of future generations of communications technologies.
- Promoting international standards and processes that are open, transparent, consensus–driven, and that do not place trusted companies at a disadvantage.
- Limiting the adoption of 5G equipment with known or suspected vulnerabilities.
- Continued engagement with the private sector on risk identification and mitigation efforts.
- Ensuring robust security capabilities for 5G applications and services.

[i] Untrusted equipment and networks are those manufactured, installed, serviced, managed, or otherwise handled by untrusted entities.

SCOPE NOTE: DHS/CISA produced this Critical Infrastructure Security and Resilience Note to provide an overview of 5G technology, and represents DHS/CISA's analysis of the vulnerabilities likely to affect the secure adoption and implementation of 5G technologies. This analysis represents the beginning of CISA's thinking on this issue, and not the culmination of it. It is not an exhaustive risk summary or technical review of attack methodologies. This product is derived from the considerable amount of analysis that already exists on this topic, to include public and private research and analysis. Analysis of complex, sophisticated, and distributed cyber intrusions against 5G networks is beyond the scope of this product. At the time of this product's creation, 5G standards, networks, and components are still under development.

This product was coordinated with the CISA Cybersecurity Division (CSD), Infrastructure Security Division (ISD), industry partners, and Sandia National Laboratories.

THE HISTORY OF CELLULAR COMMUNCIATIONS

In 1982, the first cellular wireless generation (G) in the United States launched, utilizing analog communications to provide basic speech service.[1] Since then, wireless providers have introduced new wireless generations approximately every 10 years, increasing data throughput[ii] and reducing latency[iii].[2] Digital transmission over the air, introduced in 2G, replaced analog and supported data services for mobile devices. 2G technologies enabled capabilities like text and picture messaging. Upgrades to existing networks and new mobile devices accompanied 3G's introduction, which introduced a data overlay to support data capabilities such as Global Positioning System (GPS), video conferencing, and multi-media streaming.[3,4]

4G changed the way media is consumed, enabling the wide scale transition from downloading content on home computers to streaming content on mobile devices.[5] As of June 2019, 4G is the primary wireless standard used in the United States, although 2G and 3G are still exclusively used in some rural areas that lack 4G coverage.[6,7] Two versions of 4G were released after the original standard: (LTE) and LTE Advanced (LTE-A). Both releases updated the existing 4G network and significantly improved upon its upload and download speeds.[8] 4G, however, is unable to support the needs of an evolving telecommunications industry with tens of billions of connected devices and increasing data requirements.[9] Table 1 shows the evolution of wireless generations since 1982, including the expected wide rollout of 5G.

TABLE 1—EVOLUTION OF WIRELESS GENERATIONS[10,11,12]

WIRELESS GENERATION	THROUGHPUT	LATENCY	YEAR	AMERICANS WITH MOBILE SUBSCRIPTIONS
1G	2.4 kilobits per second (kbps)	N/A	1982	<1%
2G	64 kbps	300-1000 Milliseconds (MS)	1992	3%
3G	2 Megabytes Per Second (Mbps)	100-500 MS	1998	45%
4G	100 Mbps	<100 MS	2011	96%
5G	20 Gigabytes Per Second (Gbps)	<5 MS[iv]	2020	N/A

[ii] Throughput refers to how much data can traverse from one location to another in a given amount of time.
[iii] Latency is the delay in transmitting and processing data, such as the delay between when a command is sent and when it is executed.
[iv] Emerging technologies like autonomous vehicles and remote surgery will be more feasible at these latencies.

WHAT IS 5G?

5G is the next generation of wireless technology that represents a complete transformation of telecommunication networks. Combining new and legacy technology and infrastructure, 5G will build upon previous generations in an evolution that will occur over many years, utilizing existing infrastructure and technology.

5G builds upon existing telecommunication infrastructure by improving the bandwidth, capacity, and reliability of wireless broadband services.[13] The evolution will take years, but the goal is to meet increasing data and communication requirements, including capacity for tens of billions of connected devices that will make up the Internet of Things (IoT),[v] ultra-low latency required for critical near-real time communications, and faster speeds to support emerging technologies.[14] As of June 2019, 5G networks and technologies are in development with a limited rollout in select cities around the world, including 20 in the United States.[15,16]

How Will 5G Work?

Wireless communications traditionally transmit data over low-band radio frequencies. Waves at these low-band frequencies are penetrative[vi] (can pass through walls and other materials) and can travel long distances, and therefore can use large, macro cellular towers to cover a large geographic area.[17] The 5G wireless system will transmit and receive radio signals over low-, medium-, and high-band radio frequencies (see figure 1). Expanding the range of wireless frequencies devices use will help minimize wireless traffic congestion by increasing capacity, and meet the growing requirements for greater throughput, lower latency, and higher speeds.[18] High frequency waves will improve speed but will be less penetrative and have shorter transmission ranges (likely hundreds of meters instead of kilometers). 5G will require the full complement of spectrum frequencies (low, mid, and high) because each frequency type offers unique benefits and challenges.

FIGURE 1—4G AND 5G WIRELESS FREQUENCIES[19]

In many instances, 5G will rely on a new physical architecture with components built on a system of both traditional macro cellular towers and non-traditional, smaller deployments, such as small cells and micro cells—miniature cellular towers that transmit short-range radio signals.[20] In addition to connecting directly to base stations, wireless cellular devices will be able to connect to local small cells, which will then relay data through additional small cells to macro cellular towers.[21] The architecture needed to support 5G will depend on the geography and spectrum bands utilized to provide service. In many instances, small cells will need to be deployed widely across cities to support 5G connectivity, transmitting and receiving signals from locations such as streetlights, street signs, homes, vehicles, and businesses.[22] Figure two shows 5G communication technologies and how they are connected.

[v] The connection of systems and devices with primarily physical purposes (e.g., sensing, heating and cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems. [U.S. Department of Homeland Security. (2016). "Strategic Principles for Securing the Internet of Things (IoT)." U.S. Department of Homeland Security.]

[vi] Higher frequency waves are generally unable to pass through materials, including walls and other building materials as easily as lower frequency waves.

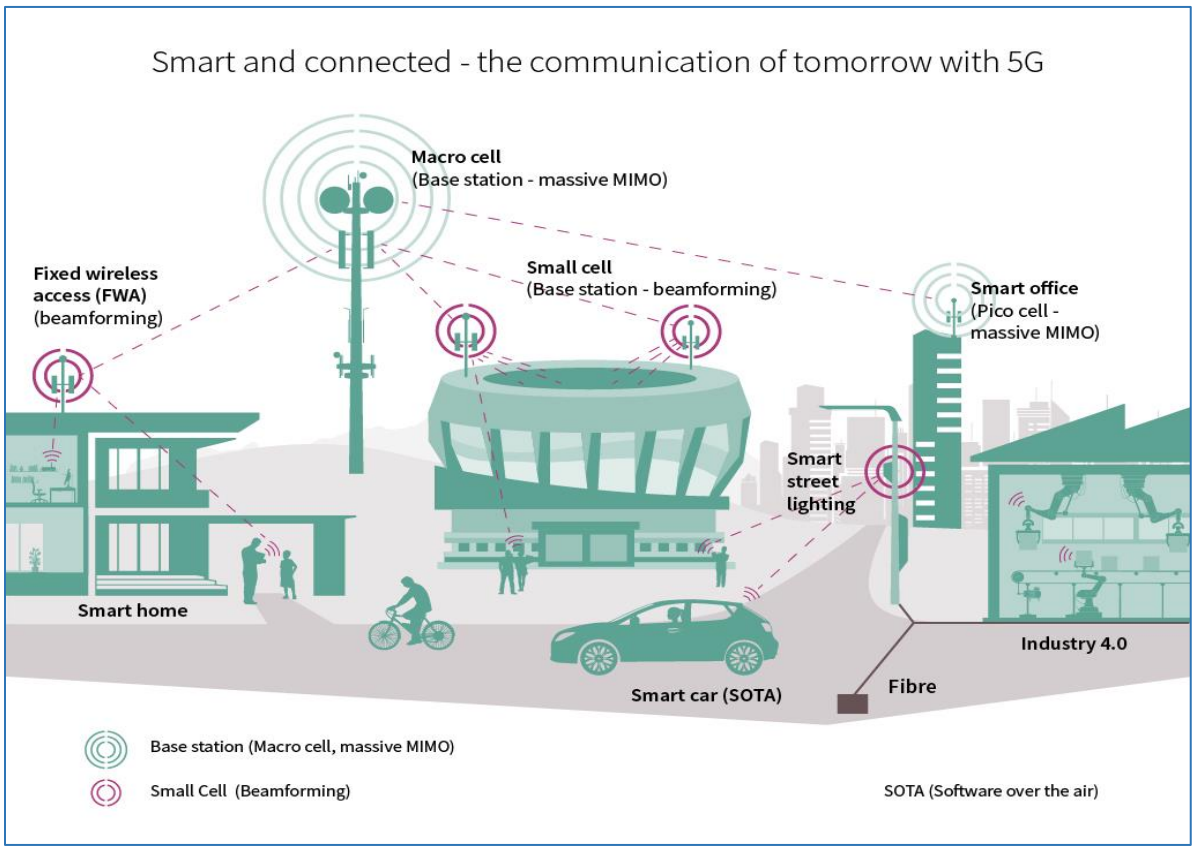


FIGURE 2—5G COMMUNICATION TECHNOLOGIES[23]

In areas with insufficient small cells to handle 5G traffic, wireless cellular devices may revert to 4G or other earlier wireless network generations. However, a lack of small cells does not mean that 5G is not possible; 5G speeds and capacity may be available through other 5G architectures. Figure three breaks down the major components of 5G networking into user equipment, radio access networks (RAN), and core network, and shows the market leaders in each area. This network architecture, with corresponding vendors, is intended to be high level. Additional granularity would result in a broader list of primary vendors, including additional American-based vendors.

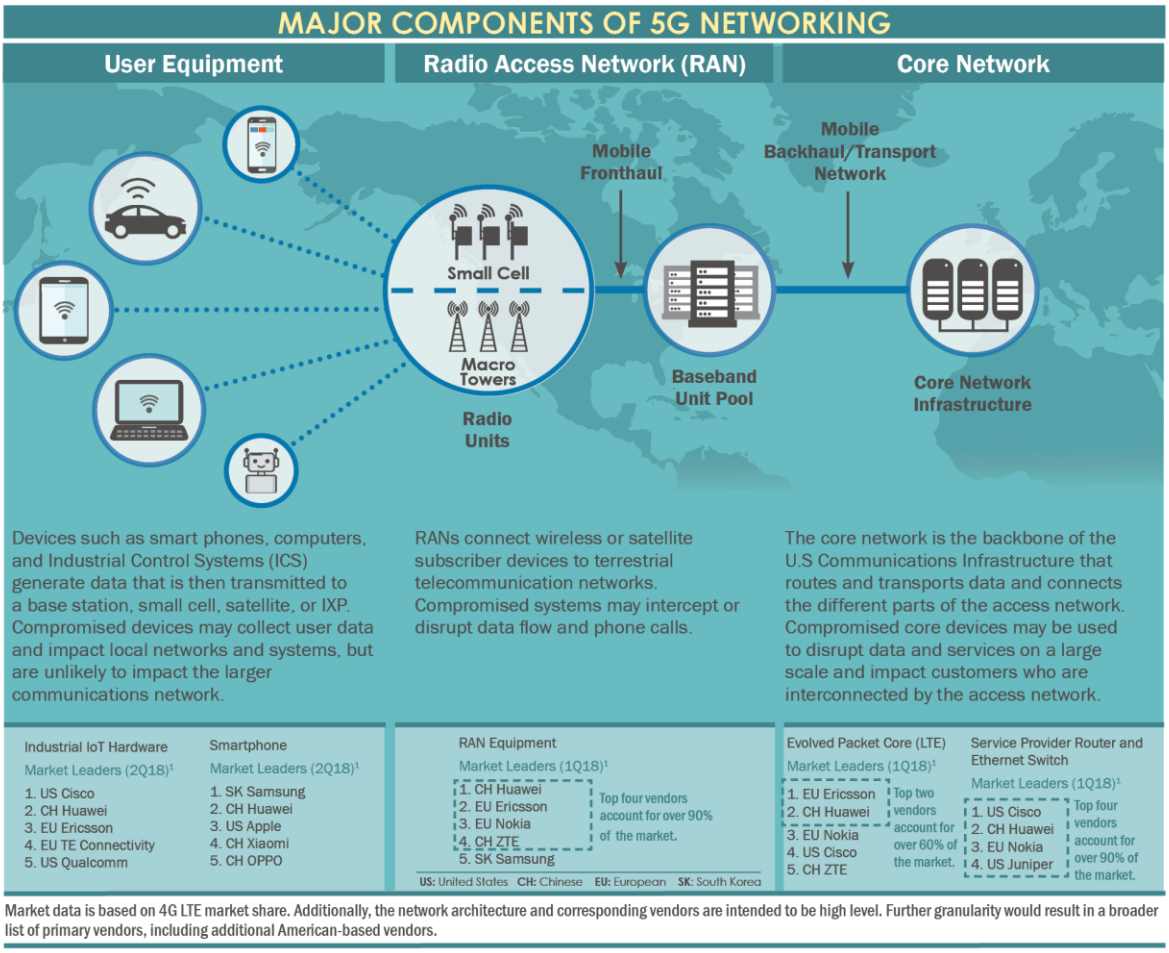


FIGURE 3—5G MAJOR COMPONENTS

How Will Technology Use 5G?

5G's higher speeds, increased bandwidth, and lower latencies will advance emerging and evolving technologies—including autonomous vehicles, augmented and virtual reality, remote medical procedures, and the IoT.[24,25,26] The low-, mid-, and high-band radio frequencies within the wireless spectrum have unique characteristics that may be utilized to meet varying use case requirements within 5G infrastructure. For example, Augmented/Virtual Reality will require high upload and download speeds, while autonomous vehicles will require ultra-low latency to ensure near-instantaneous responses. In 2016, standard and regulatory bodies categorized three primary ways[vii] technology would use 5G; Ultra-Reliable Low-Latency Communications (URLLC), Enhanced Mobile Broadband (eMBB), Massive Machine Type Communications (mMTC).[27,28,29]

[vii] Standard and regulatory bodies also identified a 4th 5G usage scenario, Network Operation, which will address system requirements, including network functions and capabilities, migration and interworking, optimizations and enhancements, and security. [3GPP (2016). "SA1 Completes its study into 5G requirements." 3GPP. http://www.3gpp.org/news-events/3gpp-news/1786-5g_reqs_sa1. Accessed on November 19, 2018.]

Table 2 summarizes the technical capabilities of each use case and provides examples of some of the technologies that will benefit.

TABLE 2—5G USE CASES[viii]

USE CASE	RADIO BAND	CAPABILITY	EXAMPLES OF 5G-ENABLED TECHNOLOGIES
eMBB	Low-Band	Low-band frequencies cover large geographic areas with penetrative signals, and can service densely populated metropolitan areas with high download speeds, likely reaching up to 20 Gbs, 20 times the speeds available from some current wireless networks.[30,31] eMBB will support data-driven applications that require high data rates across a wide coverage area, and will also support mobile connectivity, so users can access broadband consistently on the move.[32]	Augmented/Virtual Reality, Ultra High Definition Broadcasting, Home and Enterprise Broadband
URLLC	Mid-Band	Mid-band frequencies can cover large areas with the potential bandwidth to support high-capacity devices and services.[33] URLLC will support mission-critical systems and applications in which data is time-sensitive and requires high reliability.[34,35] Standard bodies have designated that end-to-end latency of 5ms or less, with an uptime of 99.999 percent.[36]	Vehicle-to-Everything (V2X)[ix], Autonomous Vehicles, Smart Grid, Tactile Feedback in Remote Medical Procedures, Unmanned Aviation, Robotics, Industrial Automation
mMTC	High-Band	High-band frequencies support fast download speeds but due to the non-penetrative signal and short range, increased infrastructure will be required to dispense signal.[37,38] mMTC will support the tens of billions of low-complexity, low-power devices that make up the IoT, and while eMBB prioritizes speed, mMTC will prioritize connectivity for a large number of devices.[39]	E-Health, Transport and Logistics, Smart Meters, Smart Agriculture

WHEN WILL 5G BE AVAILABLE?

5G began its rollout in the United States in 2018, but widespread availability is contingent on several factors, including the International Telecommunication Union's (ITU)[x] and 3rd Generation Partnership Project's (3GPP)[xi] standard finalization, federal regulation of spectrum, network implementation, and the development and production of 5G networks and devices.[40] Systems that utilize a wider range of spectrum, such as automotive and industrial automation and virtual reality, will be supported after smart phones as 5G technology and infrastructure continues to develop.[41] Widespread usage of a standalone 5G network is not expected until at

[viii] Table 2 is illustrative and is not comprehensive. Some technologies may use multiple radio bands.
[ix] V2X enables vehicles to communicate through on-board modules, small cells, road sensors, and towers.
[x] A United Nations agency responsible for Information and Communication Technologies (ICT). It allocates radio spectrum and develops global technical standards.
[xi] 3GPP is an industry based, multi-national technical organization made up of approximately 500 companies and government agencies from the U.S. Europe, China, Japan, Korea, and India.

least 2022. In the interim, the continued exponential increase of connected devices will utilize 4G, 4G LTE, and 4G/5G hybrid infrastructures for internet connectivity.

Developing 5G Standards

5G standards have addressed known security vulnerabilities from previous wireless generations and enhanced security of 5G with home routing, encryption, and network slicing[xii]. As of June 2019, Release 15 standards for 5G have been completed. Release 16 standards are expected to be finalized in December 2019 at the earliest.[42,43] 5G evolution and standard development will continue after Release 16 is completed. Standards—led by 3GPP and ITU—determine technical specifications, including spectrum bands, radio interface technologies, network architecture, and network virtualization.[44,45]

In 2015, the ITU created the International Mobile Telecommunications 2020 (IMT-2020), which detailed technical standards such as minimum speed and use cases, and designated a timeline for 5G standards development (figure 3).[46,47] 3GPP is developing and will submit candidate technologies and specifications to the IMT-2020.[48] In December 2017, 3GPP ratified the Non-Standalone (NSA)[xiii] 5G New Radio (NR) specification, which enabled vendors to start building 5G components.[49] In June 2018, the Standalone (SA)[xiv] version was completed; 5G SA defines the control plane capabilities and user specifications for the new 5G core network architecture.[50] 3GPP is targeting their final submission to IMT-2020 for the end of 2019.[51] Figure four shows the 5G standards timeline for the ITU and 3GPP.[52,53,54]

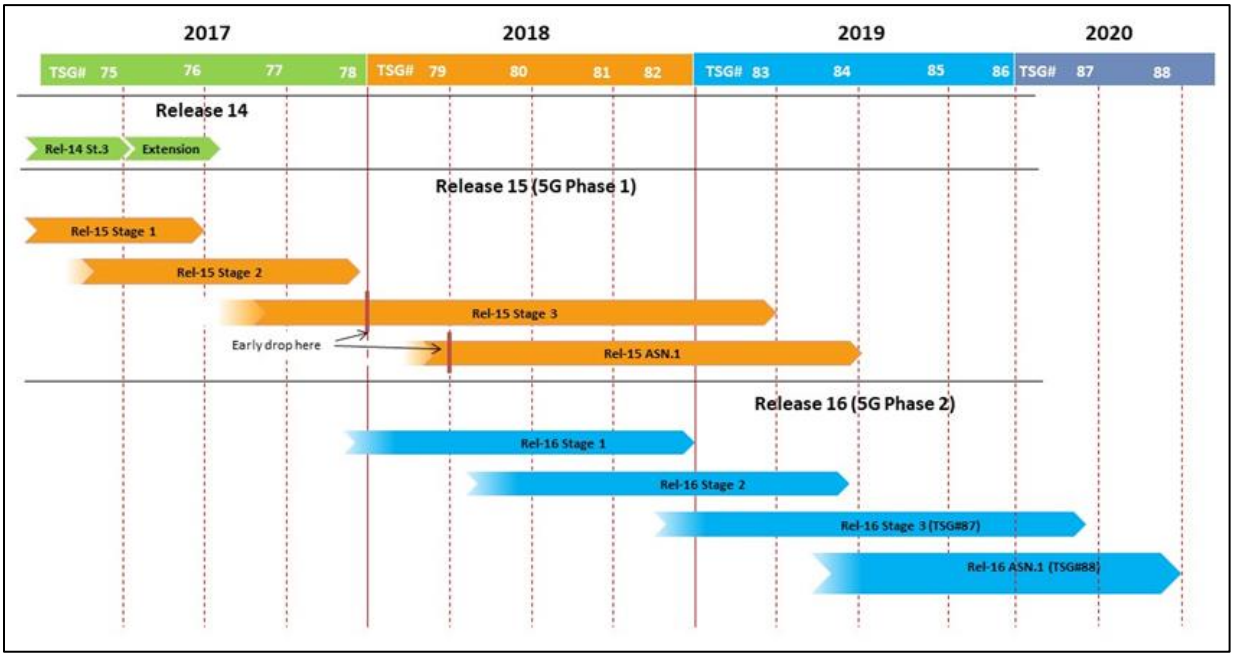


FIGURE 4—3GPP RELEASE TIMELINE AS OF JUNE 2019[55]

Federal Regulations and Activities

The Federal Communications Commission (FCC) is the U.S. Government agency that manages commercial spectrum usage.[56] The FCC has designated a large block of the underutilized high band spectrum for 5G and is auctioning 6,000 licenses in the 28 GHz and 24 GHz bands to communication companies.[57] The FCC has concluded its first high-band 5G spectrum auctions in both the 28GHz and 24GHz bands on May 28th, 2019.[58]

[xii] Network slicing will enable 5G networks to be segregated based on service or security requirements and will allow services to be created or deleted quickly.
[xiii] Non-Standalone Standards will allow devices to rest on the 4G network and will only jump up to 5G when the network is available.
[xiv] Standalone Standards will allow devices to rest on the 5G network and will only drop down when 5G is unavailable.

Additional auctions of different spectrum bands are planned for 2019. The FCC will make additional spectrum available for 5G services, to include:[59]

- **Low-band**: The FCC is acting to improve use of low-band spectrum (useful for wider coverage) for 5G services, with targeted changes to the 600 MHz, 800 MHz, and 900 MHz bands.
- **Mid-band**: Exploring, among other bands, a shared service framework in the 3.5 GHz band and developing next steps for terrestrial use in the 3.7 GHz band.
- **High-band**: Releasing spectrum at the frontiers of the spectrum chart, including spectrum auctions in the 24 and 28 GHz bands, and 2019 auctions planned in the 37, 39, and 47 GHz bands with additional bands still being explorer for potential terrestrial wireless use.[60]

A key venue for collaborative work between government and the private sector is the FCC's Communications Security, Reliability and Interoperability Council (CSRIC). The CSRIC is a federal advisory committee made up of members from both the private sector and government. Its mission is to provide recommendations to the FCC to ensure, among other things, security and reliability of communications systems, including telecommunications, media, and public safety. DHS participates in CSRIC efforts on cybersecurity and communications network security, complementing DHS' role as the sector-specific agency for the communications sector.

5G Deployment in the United States

As of June 2019, 5G networks and technologies are still in development and have rolled out on a limited basis in cities.[61] The full benefits of 5G may not be available during this initial deployment, either because users do not have 5G enabled devices that can use the 5G networks, or because there is inadequate base infrastructure for 5G enabled devices to access.[62]

One U.S. carrier deployed a fixed 5G network to four U.S. cities in October 2018, which will have the benefits of 5G signal but will not provide mobile access to a 5G network.[63] This home broadband service is a pre-standards deployment and does not meet the globally recognized 5G standard, although the company says it will adopt the industry standard in 2019 while it rolls out 5G mobile service for phones. A second U.S. carrier deployed a mobile 5G network in 12 U.S. cities in December 2018, although limited availability 5G mobile hotspots are the only devices capable of using the 5G network; 5G capable smartphones are expected to be available in 2019. Two additional U.S. carriers are targeting 2020 for full nationwide 5G coverage with limited rollouts beginning in 2019.[64,65] Many of these devices are enabled by a 5G modem developed by a leading U.S. chip manufacturer, which 18 international Original Equipment Manufacturer (OEM) companies and 19 wireless network operators have committed to using in trials.[66]

5G VULNERABILITIES

The move to 5G presents opportunities to enhance security and create a better user experience; however, it may result in vulnerabilities related to supply chains, deployment, network security, and the loss of competition and choice. While not all inclusive, there are a range of vulnerabilities that could increase risk for the United States as the country's networks migrate to 5G, including: reliance on untrusted entities and the global supply chain, lack of participation by untrusted companies in interoperability efforts, increased size of 5G infrastructure, integration within existing vulnerable networks, and untrusted company development of custom code for ICT components.

Supply Chain

USE OF 5G COMPONENTS MANUFACTURED BY UNTRUSTED COMPANIES COULD EXPOSE U.S. ENTITIES TO RISKS INTRODUCED BY MALICIOUS SOFTWARE AND HARDWARE; COUNTERFEIT COMPONENTS; AND COMPONENT FLAWS CAUSED BY POOR MANUFACTURING PROCESSES AND MAINTENANCE PROCEDURES.

Though equipment designed and manufactured by trusted suppliers is not immune to manipulation, equipment produced or otherwise handled by untrusted partners presents more risk of malicious or inadvertent introduction of vulnerabilities. Counterfeit components and the insertion of malicious software and hardware are a few examples of such vulnerabilities. Even if ICT components are purchased from trusted companies, the company may maintain production facilities overseas which may be vulnerable to supply chain risk.

Compromised components could affect network performance and compromise the confidentiality, integrity, and availability of network assets. Furthermore, compromised devices may provide malicious actors with persistent access to 5G networks and the capability to intercept data that routes through the devices. Compromised devices may infect connected computers, phones, and other devices with malware and may have data rerouted, changed, or deleted.

Untrusted companies that have significant international market share within telecommunication networks may introduce risks even if they do not have a large presence within the U.S networks. Therefore, even if the U.S. network were completely secure, data traveling overseas may pass through untrusted telecommunication networks and potentially be vulnerable to interception, manipulation, disruption, or destruction.

Network Security

DESPITE SECURITY ENHANCEMENT OVER PREVIOUS GENERATIONS, IT IS UNKNOWN WHAT NEW VULNERABILITIES MAY BE DISCOVERED IN 5G NETWORKS.

Component manufacturers and service providers are developing technologies and security specifications to mitigate vulnerabilities in wireless networks. 5G will push ICT components and data management to the edge of the network, which will enhance security through network slicing, edge computing power, device management, authentication functions, and automated threat detection and response. Network slicing, if implemented properly, should limit an attacker's ability to access critical areas within a network. The migration of functions to the edge of the network will increase computing and network management power, which will secure traffic and prevent intrusions to core network systems.

Despite 5G's security improvements, as with all new technologies it is likely that 5G equipment and protocols will inadvertently contain vulnerabilities that could expose components and data to exploitation. Even as security updates are released, some entities may be slow to implement them for a variety of reasons, such as the potential impact to operations from taking systems offline. Therefore any vulnerabilities inherent in 5G technologies may be exploitable even after fixes are developed.

5G BUILDS UPON PREVIOUS GENERATIONS OF WIRELESS NETWORKS AND WILL INITIALLY BE INTEGRATED WITH 4G LTE NETWORKS THAT CONTAIN SOME LEGACY VULNERABILITIES, POTENTIALLY INCLUDING UNTRUSTED COMPONENTS.

5G network technologies are being designed to be more secure than previous mobile network generations, and organizations and standard bodies continue to enhance security in previous wireless networks, including protecting core networking systems from malicious edge networking devices. 5G technologies will, however, initially be overlaid on the existing 4G Long-Term Evolution (LTE) network that contains legacy vulnerabilities. These could be inadvertent, technical vulnerabilities inherent to the network, or due to 5G technologies' integration into untrusted 4G and 4G LTE networks. The inheritance of security settings, permissions, and technical specifications from an untrusted core network may negate built-in 5G device security.

5G Deployment

THE PROLIFERATION OF 5G NETWORKS COULD PROVIDE MALICIOUS ACTORS MORE ATTACK VECTORS TO INTERCEPT, MANIPULATE, DISRUPT, AND DESTROY CRITICAL DATA.

5G will use more components than previous generations of wireless networks and malicious actors may have addtional vectors to intercept, manipulate, disrupt, and destroy critical data. This infrastructure will likely include, but is not limited to cellular towers, beamforming, small cells, and mobile devices.

Unlike traditional cellular towers, small cells will be densely deployed in metropolitan areas, residing on light poles, trees, homes, building corners, and retail shops.[67] Although small cells are designed with physical security features, they still could be compromised through physical access. This may provide malicious actors with persistent illicit access to the 5G network, the ability to intercept data routed through the device, and an avenue to conduct Denial of Service (DOS) attacks on devices communicating with that small cell. Compromised small cells may also provide malicious actors the capability to clone devices, allowing the replica to make calls, use data, and add charges.

While the use of small cells for information extraction or disruption is possible, the use of such a method would likely require a high level of sophistication and is unlikely to provide access to large volumes of data. As of June 2019, there are no confirmed incidents utilizing 5G small cells to exploit wireless systems, however, researchers have demonstrated this capability with small cells in a 4G wireless system.

- In 2013, a pair of security researchers detailed their ability to use a small cell to intercept voice calls, data, and SMS text messages of any handset that connects to the device. The security researchers also demonstrated the ability to clone a cell phone, allowing hackers to impersonate the device to make calls, send texts, and use data.[68]

THE EFFECTIVENESS OF 5G SECURITY ENHANCEMENTS WILL IN PART DEPEND ON PROPER IMPLEMENTATION AND CONFIGURATION.

Advanced security features in 5G protocols and technologies will improve communications security but will require proper configuration and implementation. As municipalities, companies, and organizations build their own local 5G networks, it is possible they will not properly implement 5G network security. Improperly deployed, configured, or managed 5G equipment and networks may be vulnerable to interception, disruption, and manipulation.

Loss of Competition and Trusted Options

UNTRUSTED COMPANIES MAY BE LESS LIKELY TO PARTICIPATE IN INTEROPERABILITY EFFORTS, POTENTIALLY MAKING IT DIFFICULT FOR TRUSTED COMPANIES TO COMPETE AND LIMITING THE AVAILABILITY OF TRUSTED COMMUNICATIONS TECHNOLOGIES.

Section 889 of the 2019 National Defense Authorization Act (NDAA) prohibits federal agencies from procuring certain equipment and services from Huawei and ZTE, two of the world's largest manufacturers of telecommunications equipment.[69] Although limited in their share of the U.S. telecommunications market, these companies have significant market share internationally and may be less likely to participate in interoperability efforts. This is evidenced by the lack of involvement in the O-RAN Alliance, a collection of telecommunication organizations that work towards open and interoperable architectures.[70]

Communication network operators that previously purchased 4G equipment from a company like Huawei that uses proprietary interfaces in their technologies cannot easily use other vendors' equipment for 5G. The proprietary interfaces lock customers into a single vendor procurement cycle, which could negatively affect competitive balance within the 5G market. Loss of market share could limit trusted companies' ability to invest in research and development and could eventually drive them out of the market. Loss of trusted suppliers could potentially lead to a situation where untrusted entities are the only options.

CUSTOM 5G TECHNOLOGIES THAT DO NOT MEET INTEROPERABILITY STANDARDS MAY BE MORE DIFFICULT TO UPDATE AND REPAIR, POTENTIALLY INCREASING THE LIFECYCLE COST OF THE PRODUCT.

Custom 5G equipment, that does not meet interoperability standards, may be more difficult to update and repair. Poorly developed code makes vulnerability management significantly more difficult and can lead to unsupportable software. If a critical outage occurs, systems, programs, and data with custom code are more difficult to recover and may lead to extended outage times.

Slowing or blocking interoperability between networks could also substantially delay or increase the cost of deploying 5G. A customer currently using Huawei equipment who wants to use a new vendor for 5G may have to first remove and replace all their equipment from the network.

Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report

On March 28, 2019, the British National Cyber Security Centre (NCSC) released an assessment on the security risks posed by Huawei. The report identified "significant, concerning issues in Huawei's approach to software development, which brings significantly increased risk to UK operators, and requires ongoing management and mitigation." The report also states that "The Oversight Board continues to be able to provide only limited assurance that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK."

NATIONAL OPPORTUNITIES TO MITIGATE 5G RISK

With the above in mind, there is an opportunity for the U.S. government and industry to work together to maximize the benefits of next generation communication networks and to promote security and resilience associated with emerging 5G technologies. Given the expected rollout schedule, 2019 presents a window of time in which the United States and allied countries can advance risk mitigation efforts that may be more difficult to address as the deployment of 5G networks advance. The below presents a range of opportunities at the strategic level. Follow on efforts and discussions are necessary to expand on specific potential actions.

Encouraging continued trusted development of 5G technologies, services, and products

Reliance on untrusted 5G technologies is likely, in part, because of relatively low costs. Additionally, if untrusted companies' equipment is already installed as part of the 4G LTE network, lack of interoperability may make it impossible to install other companies' 5G equipment without replacing the existing 4G LTE equipment, which may be extremely costly. National investment in research and development, economic incentives for manufacturing and buying trusted components, or economic deterrents for purchasing and installing untrusted components, could increase trusted production and lower the risks of malicious untrusted technologies.

Encouraging continued trusted development of the next generations of communications technologies

Next generation communication technologies and standards will build upon themselves over time and security enhancements will continue for 5G into the future. This development will occur in individual companies and in standards bodies as markets for new services take shape, but the United States can encourage and investin in such development. This will likely position the United States to be a leading player in their rollout, potentially decreasing the influence of adversarial nations and decreasing U.S. reliance on untrusted technologies.

Promoting international standards and processes that are open, transparent, and consensus-driven and that do not place trusted companies at a disadvantage

The ITU and 3GPP both have U.S. members, including the director of ITU's Telecommunication Development Bureau, one of ITU's five top elected officials serving 2019-2022.[71] Members of the two groups representing trusted suppliers' interests can promote standards that are currently being adopted and collaborate on their development. The United States could also work at achieving greater representation in the ITU, 3GPP, and other standard organizations.

Limiting the use of 5G equipment with known or suspected vulnerabilities

The United States can take action to limit the adoption of 5G equipment that may contain vulnerabilities. For example, Section 889 of the 2019 NDAA prohibits federal agencies from procuring certain telecommunications equipment and services. The recently enacted Federal Acquisition Supply Chain Security Act provides the government with important new authorities. These authorities address risks presented by the purchase of technologies developed or supplied by entities whose manufacturing and development processes, obligations to foreign governments, and other factors raise supply chain concerns.[72] In May 2019, the President also issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain, which authorizes the Secretary of Commerce, in consultation with other agencies, to issue regulations to address the installation and use of information and communications technology and services, by any person subject to the jurisdiction of the United States, that present security risks. The United States can help secure its overseas communications by working with international partners to limit the installation of untrusted equipment abroad. The United States can also promulgate and promote technical best practices for mitigating aspects of 5G risk.

Continued engagement with the private sector on risk identification and mitigation efforts

The U.S. Government can continue to work with the private sector—to include information and communication technology providers—to help mitigate vulnerabilities. The private sector can provide insights on where government support or intervention—such as through the development of best practices, the convening of industry and government partners, and the prohibition on untrusted equipment—will help secure 5G technologies and the 5G network.

Ensure robust security capabilities for 5G applications and services

The U.S. Government and industry partners can develop security capabilities that protect not only the 5G infrastructure, but also the applications and services that utilize it. The U.S. Government can do this by incorporating a prevention-focused approach that focuses on visibility and security across the mobile network. Secure 5G applications and services will likely mitigate the risk of malware being transported across protected devices and defend against unauthorized command and control from exploited connected devices. The U.S. Government and its industry partners can also encourage secure infrastructure to guard against these threats and mitigate lateral threat movement within the 5G network.

GLOSSARY OF TERMS

TERM	DESCRIPTION
3rd Generation Partnership Project (3GPP)	3GPP is an industry based, multi-national technical organization made up of approximately 500 companies and government agencies from the U.S. Europe, China, Japan, Korea, and India.
Baseband Unit Pool (BBU)	BBUs are the baseband processing units within telecom systems that comprise cloud radio access networks (C-RAN). BBUs are located at centralized sites and function as a cloud or a data center.
Beamforming	Beamforming is a radio frequency management function in which radio access locations use multiple antennas to focuses radio signals in a specific direction. This enhances the uplink and downlink capabilities as well as the overall network capacity of the signal.
Communications Security, Reliability and Interoperability Council (CSRIC)	CSRIC is a joint federal and industry partnership that aims to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.
Device-To-Device (D2D)	D2D is a communication technology that enables direct data transfer between nearby mobile devices in an ad-hoc network. Devices would act as data transfer points, relaying data between end users, small cells, and base stations.[73]
Internet of Things (IoT)	The connection of systems and devices with primarily physical purposes (e.g., sensing, heating and cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems
International Telecommunications Union (ITU)	A United Nations agency responsible for information and communication technologies. It allocates radio spectrum and develops global technical standards.
Latency	The delay in transmitting and processing data, such as the delay between when a command is sent and when it is executed.
Macro Cell	Macro cell towers reside on a base station and deliver wireless radio signal in a large geographic area. 5G macro cells will operate in similar frequency bands as 4G Long-Term Evolution (LTE).
Machine-To-Machine (M2M)	M2M communication occurs between two directly connected machines without human interference. M2M will support 5G use cases; including the large number of low-cost/low-energy IoT devices, as well as enabling critical machine type communications in smart factory, automotive, and e-health systems.
Massive MIMO (Multiple-Input, Multiple-Output)	Massive MIMO technology increases the capabilities of wireless internet by putting significantly more antennae on a base station. 4G base stations have twelve antennae, whereas 5G massive MIMO base stations can support an estimated one hundred antennae, increasing capacity of mobile networks by a factor of 22 or greater.[74]

Mobile Backhaul	Mobile Backhaul is the back-end part of a cellular network that connects the edge or fronthaul networks to the core network via fiber optic cables.
Mobile Fronthaul	Mobile Fronthaul is the front-end or edge interfacing portion of the cellular network that connects the radio access network to the mobile backhaul network via fiber optic cables.
Small Cell/Micro Cell	A small cell is miniature base station that transmits short-range radio signals. Due to the limited range and non-penetrative signal of high frequency radio wave bands, 5G will require numerous small cells to support its infrastructure. Together, these cells would form a dense network that relays data through multiple small cells.[75]
Vehicle-To-Everything (V2X)	Similar to D2D, V2X is a communication technology in which vehicles act as data relay points between 5G enabled vehicles, end-user devices, and smart city components like smart sensors or meters.
Wave Penetration	The ability to pass through materials, such as walls. Waves at low-band frequencies are generally penetrative, while higher frequency waves are often unable to pass through materials, including walls and other building materials.

The National Risk Management Center (NRMC), Cybersecurity and Information Security Agency (CISA), is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. All NRMC products are visible to authorized users at HSIN-CI and Intelink. For more information, contact NRMC@hq.dhs.gov or visit https://www.dhs.gov/cisa/national-risk-management-center.

[1] Segan, S. (2015). "3G vs. 4G: What's the Difference?" PC Mag. https://www.pcmag.com/article2/0,2817,2399984,00.asp. Accessed on June 5, 2019.
[2] Sharma, P. (2013). "Evolution of Mobile Wireless CommunicationNetworks-1G to 5G as well as Future Prospective of Next Generation Communication Network." International Journal of Computer Science and Mobile Computing.
[3] Rouse, M. (2009). "3G (third generation of mobile telephony)." Tech Target. https://searchtelecom.techtarget.com/definition/3G. Accessed on June 5, 2019.
[4] Thangham, Chris. (2008). "New Apple iPhone will have 3G, GPS, Video Conferencing, Live TV, more memory, colors." Digital Journal. http://www.digitaljournal.com/article/254685. Accessed on June 5, 2019.
[5] Granados, N. (2017) "5G: The Next Tech Disruption In Media And Entertainment Is Coming." Forbes. https://www.forbes.com/sites/nelsongranados/2017/07/17/5g-the-next-tech-disruption-in-media-and-entertainment-is-coming/#4bc886037026. Accessed on June 5, 2019.
[6] Nperf. (2018). "2G/3G/4G coverage map, United States." https://www.nperf.com/en/map/US/-/-/signal/. Accessed on June 5, 2019.
[7] Segan, S. (2018). "Fastest Mobile Networks 2018." PC Mag. https://www.pcmag.com/Fastest-Mobile-Networks/4. Accessed on June 5, 2019.
[8] Segan, S. (2015). "3G vs. 4G: What's the Difference?" PC Mag. https://www.pcmag.com/article2/0,2817,2399984,00.asp. Accessed on June 5, 2019.
[9] Fisher, T. (2018). "How are 4G and 5G Different?" Lifewire. https://www.lifewire.com/5g-vs-4g-4156322. Accessed on June 5, 2019.
[10] Phone Arena. (2013). "1G, 2G, 3G, 4G: The evolution of wireless generations." https://www.phonearena.com/news/1G-2G-3G-4G-The-evolution-of-wireless-generations_id46952. Accessed on June 5, 2019.
[11] Grigorik, I. (2013). "High Performance Browser Networking." https://hpbn.co/#toc. Accessed on June 5, 2019.
[12] Intel. (2014) "The Evolution of Wireless Technology." http://download.intel.com/newsroom/kits/atom/comms/pdfs/Final-EvolutionOfWireless.pdf. p. 1. Accessed on June 5, 2019.

[13] Downes, L. (2018). "5G: What is it good for?" Washington Post. https://www.washingtonpost.com/news/innovations/wp/2018/06/05/5g-what-is-it-good-for/?utm_term=.681b76b740ff. Accessed on June 5, 2019.
[14] Wired. (2018). "What is 5G, and When Do I Get it?" https://www.wired.com/2017/02/what-is-5g-and-when-do-i-get-it/. Accessed on June 5, 2019.
[15] Garcia, A. (2019). "Looking for 5G? Here are the US Cities that have it." https://www.cnn.com/2019/04/09/tech/5g-network-us-cities/index.html. Accessed on June 4, 2019.
[16] Blumenthal, Eli. (2018). "AT&T turns on its mobile 5G network on Dec. 21, starting with 12 cities and mobile hotspot." USA Today. https://www.usatoday.com/story/tech/2018/12/18/att-opens-its-5-g-network-december-21-starting-12-cities/2339042002/. Accessed June 5, 2019.
[17] Greenemeier, L. (2015). "Will Millimeter Waves Maximize 5G Wireless?" Scientific American. https://www.scientificamerican.com/article/will-millimeter-waves-maximize-5g-wireless/. Accessed June 5, 2019.
[18] Valdez, D. (2019). "5G expected to ease network congestion." Business World. https://www.bworldonline.com/5g-expected-to-ease-network-congestion/. Accessed on June 4, 2019.
[19] Moorhead, Patrick (2016) "Qualcomm Demonstrates First Sub-6 GHz 5G New Radio Prototype At MWC Shanghai 2016" https://www.forbes.com/sites/patrickmoorhead/2016/06/26/qualcomm-demonstrates-first-sub-6-ghz-5g-new-radio-prototype-at-mwc-shanghai-2016/#7a8b45fd194b. Accessed on June 12, 2019.
[20] FCC. (2018). "The FCC's 5G FAST Plan." https://www.fcc.gov/5G. Accessed on June 5, 2019.
[21] Nordrum, A, Clark, K. (2018). "5G Bytes: Small Cells Explained." IEEE. https://spectrum.ieee.org/video/telecom/wireless/5g-bytes-small-cells-explained. Accessed on June 5, 2019.
[22] Ibid.
[23] Infineon (2017) "Infineon RF solutions for fast, efficient and reliable 5G" https://www.infineon.com/cms/en/about-infineon/press/market-news/2017/INFPMM201702-034.html. Accessed on June 12, 2019.
[24] Athow, D. (2018). "5G to Open Up New Healthcare Possibilities." Tech Radar. https://www.techradar.com/news/5g-to-open-up-new-healthcare-possibilities. Accessed on June 5, 2019.
[25] Electric Light & Power. (2017) "5G Communication to Enhance Power Grid Networking." Electric Light & Power. https://www.elp.com/articles/2017/12/5g-communications-to-enhance-power-grid-networking.html. Accessed on June 5, 2019.
[26] Nichols, M. (2017). "Why 5G Will Disrupt the Robotics and Manufacturing Industries?" Robotics Business Review. https://www.roboticsbusinessreview.com/manufacturing/will-5g-disrupt-robotics-manufacturing-industries/. Accessed on June 5, 2019.
[27] 3GPP (2016). "SA1 Completes its study into 5G requirements." 3GPP. http://www.3gpp.org/news-events/3gpp-news/1786-5g_reqs_sa1. Accessed on June 5, 2019.
[28] Sagam, P. (2018). "What is the killer use case for 5G?" Forbes. https://www.forbes.com/sites/forbescommunicationscouncil/2018/06/04/what-is-the-killer-use-case-for-5g/. Accessed on June 5, 2019.
[29] Kavanagh, S. (2018). "What is enhanced Mobile Broadband (eMBB)." 5G.CO.UK. https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/. Accessed on June 5, 2019.
[30] Kavanagh, S. (2018). "What is enhanced Mobile Broadband (eMBB)." 5G.CO.UK. https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/. Accessed on June 5, 2019.
[31] Wang, B. (2015). "5G network defined by ITU as 20 GBs per second." Next Big Future. https://www.nextbigfuture.com/2015/06/5g-network-defined-by-itu-as-20-gbs-per.html. Accessed on June 5, 2019.
[32] Kavanagh, S. (2018). "What is enhanced Mobile Broadband (eMBB)." 5G.CO.UK. https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/. Accessed on June 5, 2019.
[33] Layton, R. (2018). "The U.S. Must Move Quickly On Mid-Band Spectrum If It Wants To Lead In 5G." Forbes. https://www.forbes.com/sites/roslynlayton/2018/05/23/the-us-must-move-quickly-on-mid-band-spectrum-if-it-wants-to-lead-in-5g/#fb740c67462a. Accessed on June 5, 2019.
[34] Popovski, P. Nielsen, J.Stefanovic, C. Carvalho, E.Stro¨my, E. Trillingsgaard, K. Bana, A. Kim, D. Kotaba, R. Park, J. Sørensen, R. "Wireless Access for Ultra-Reliable Low-Latency Communication (URLLC): Principles and Building Blocks." https://arxiv.org/pdf/1708.07862.pdf. p. 1. Accessed on June 5, 2019.
[35] Fulton, S. (2018). "What is 5G? The definitive guide to next generation wireless technology." ZDNet. https://www.zdnet.com/article/what-is-5g-everything-you-need-to-know/. Accessed on June 5, 2019.
[36] McLaughlin, R. (2019). "5G Low Latency Requirements". Broadband Library. https://broadbandlibrary.com/5g-low-latency-requirements/. Accessed on June 5, 2019.
[37] Brodkin, J. (2018). "AT&T's 5G trials produce gigabit speeds and 9ms latency." Arstechnica. https://arstechnica.com/information-technology/2018/04/atts-5g-trials-produce-gigabit-speeds-and-9ms-latency/. Accessed on June 5, 2019.
[38] Small Cell Forum. (2018). "MMwave small cells boost capacity tenfold, but where are the use cases?" https://www.smallcellforum.org/blog/mmwave-small-cells-boost-capacity-tenfold-use-cases/. Accessed on June 5, 2019.
[39] Bockelmann, C. Pratas, N. Nikopour, H. Au, K. Svensson, T. Stefanovic, C. Popovski, P. Dekorsy, A. (2017). "Massive Machine-type Communications in 5G." https://arxiv.org/ftp/arxiv/papers/1606/1606.03893.pdf. pp.1-2. Accessed on June 5, 2019.
[40] McGarry, C. (2019). "The Truth About 5G: What's Coming (and What's Not) in 2019". Tom's Guide. https://www.tomsguide.com/us/5g-release-date,review-5063.html. Accessed on June 5, 2019.
[41] Jones, Dan. (2019). "A 5G Device Timeline for 2018 & Beyond" https://www.lightreading.com/mobile/5g/a-5g-device-timeline-for-2018-and-beyond/d/d-id/745191. Accessed on June 5, 2019.
[42] 3GPP. (2019). "Release 15". 3GPP. https://www.3gpp.org/release-15. Accessed on June 5, 2019.
[43] 3GPP. (2018). "Release 16". 3GPP. https://www.3gpp.org/release-16. Accessed on June 5, 2019.
[44] 3GPP. (2016). "3GPP on Track to 5G." http://www.3gpp.org/news-events/3gpp-news/1787-ontrack_5g. Accessed on July 5, 2018.
[45] Gutierrez, P. Haeffner, W. (2017). "Service Function Chaining Dataplane Elements in Mobile Networks." IETF. https://tools.ietf.org/id/draft-aranda-sfc-dp-mobile-03.txt. Accessed on June 5, 2019.
[46] Blanchard, N. (2017). "How ITU, 5GPPP, NGMN and others will create the standard for 5G." Fierce Wireless. https://www.fiercewireless.com/special-report/how-itu-5gppp-ngmn-and-others-will-create-standard-for-5g. Accessed on June 5, 2019.
[47] ITU-R. (2015). "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond." https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf. p. 4-21. Accessed on June 5, 2019.
[48] Flore, D. (2015). "Tentative 3GPP timeline for 5G." 3GPP. http://www.3gpp.org/news-events/3gpp-news/1674-timeline_5g. Accessed on June 5, 2019.
[49] Alleven, M. (2017). "3GPP declares first 5G NR spec complete." Fierce Wireless. https://www.fiercewireless.com/wireless/3gpp-declares-first-5g-nr-spec-complete. Accessed on June 5, 2019.

[50] 3GPP. (2018). "Rel-15 success spans 3GPP groups." http://www.3gpp.org/news-events/3gpp-news/1965-rel-15_news. Accessed on June 5, 2019.
[51] 3GPP. (2018). "Release 16." http://www.3gpp.org/release-16. Accessed on June 5, 2019.
[52] Flore, D. (2015). "Tentative 3GPP timeline for 5G." http://www.3gpp.org/news-events/3gpp-news/1674-timeline_5g. Accessed on June 5, 2019.
[53] Johnson, D. (2018). "5G Poised for Commercial Rollout by 2020." IEEE. https://spectrum.ieee.org/tech-talk/telecom/wireless/5g-is-meeting-its-targets-for-2020-commercial-rollout. Accessed on June 5, 2019.
[54] SDX Central. "5G Standards: What You Need to Know." SDX Central. https://www.sdxcentral.com/5g/definitions/5g-standards/. Accessed on June 5, 2019.
[55] Netmanis (2017) "Timeline of 5G in ITU-R and 3GPP" https://www.netmanias.com/en/post/oneshot/11147/5g/timeline-of-5g-standardization-in-itu-r-and-3gpp. Accessed June 4, 2019.
[56] FCC (2019). "Radio Spectrum Allocation." FCC. https://www.fcc.gov/engineering-technology/policy-and-rules-division/general/radio-spectrum-allocation. Accessed on June 4, 2019.
[57] FCC. (2018). "FCC Public notice" FCC. https://docs.fcc.gov/public/attachments/FCC-18-109A1_Rcd.pdf/. Accessed on June 4, 2019.
[58] FCC. (2018). ""FCC concludes first High-Band 5G Airwaves Auctions". FCC. https://docs.fcc.gov/public/attachments/DOC-357702A1.pdf. Accessed on June 4, 2019.
[59] FCC. (2018). "The FCC's 5G FAST Plan." https://www.fcc.gov/5G. Accessed on June 5, 2019.
[60] FCC. (2018). "FCC's First-Ever High-Band 5G Spectrum Auction Begins Today." https://docs.fcc.gov/public/attachments/DOC-355073A1.pdf. Accessed June 5, 2019.
[61] Blumenthal, Eli. (2018). "AT&T turns on its mobile 5G network on Dec. 21, starting with 12 cities and mobile hotspot." USA Today. https://www.usatoday.com/story/tech/2018/12/18/att-opens-its-5-g-network-december-21-starting-12-cities/2339042002/. Accessed June 5, 2019.
[62] McGarry, C. (2018). "The Truth About 5G: What's Coming (and What's Not) in 2018." Tom's Guide. https://www.tomsguide.com/us/5g-release-date,review-5063.html. Accessed on June 5, 2019.
[63] Ibid
[64] AT&T. (2018). "AT&T First to Make Mobile 5G Service Live in the U.S. on Dec. 21." AT&T. https://about.att.com/story/2018/att_brings_5g_service_to_us.html. Accessed June 5, 2019.
[65] Cheng, R. (2018). "Sprint targets first mobile 5G nationwide network by early 2019." CNet https://www.cnet.com/news/sprint-targets-first-mobile-5g-nationwide-network-by-early-2019/. Accessed on June 5, 2019.
[66] Michaels, P. (2018). "Qualcomm's Blazing 5G Modem Coming to Phones in 2019." Tom's Guide. https://www.tomsguide.com/us/qualcomm-x50-5g-modem,news-26584.html. Accessed on June 5, 2019.
[67] Wall, M. (2018). "What is 5G and what will it mean for you?" BBC. https://www.bbc.com/news/business-44871448. Accessed on June 5, 2019.
[68] Couts, A. (2013). "Meet the $250 Verizon device that lets hackers take over your phone." Digital Trends. https://www.digitaltrends.com/mobile/femtocell-verizon-hack/. Accessed on June 5, 2019.
[69] 115th Congress. (2017). "H.R.2810 - National Defense Authorization Act for Fiscal Year 2018." https://www.congress.gov/bill/115th-congress/house-bill/2810/text. Accessed on June 5, 2019.
[70] O-RAN Alliance (2019). "Operator Defined Next Generation RAN Architecture and Interfaces". ORAN. https://www.o-ran.org/. Accessed on June 5, 2019.
[71] ITU. (2019). "ITU Management Team 2019-2022." https://www.itu.int/en/osg/Pages/itu-management-team.aspx. Accessed on June 5, 2019.
[72] 115th Congress. (2017). "H.R.2810 - National Defense Authorization Act for Fiscal Year 2018." https://www.congress.gov/bill/115th-congress/house-bill/2810/text. Accessed on June 5, 2019.
[73] IEEE Spectrum. (2018). "Applications of Device-to-Device Communication in 5G Networks." https://spectrum.ieee.org/computing/networks/applications-of-devicetodevice-communication-in-5g-networks. Accessed on June 5, 2019.
[74] Ibid.
[75] Nordrum, A, Clark, K. (2018). "5G Bytes: Small Cells Explained." IEEE. https://spectrum.ieee.org/video/telecom/wireless/5g-bytes-small-cells-explained. Accessed on June 5, 2019.

Appendix 4

Executive Order 13873 Response - Methodology For Assessing The Most Critical Information And Communications Technologies And Services, CISA, April 2020

EXECUTIVE ORDER 13873 RESPONSE

METHODOLOGY FOR ASSESSING THE MOST CRITICAL INFORMATION AND COMMUNICATIONS TECHNOLOGIES AND SERVICES

April 2020

CISA
CYBER+INFRASTRUCTURE

This page is intentionally left blank.

KEY FINDINGS

- The Cybersecurity and Infrastructure Security Agency's (CISA) National Risk Management Center (NRMC) identified 61 Information and Communication Technology (ICT) elements organized into five roles (Local User Access, Transmission, Storage, Processing, and System Management) and 11 sub-roles.
- The 11 sub-roles are:
    - Broadcast Networks
    - Wireless Local Area Networks
    - Mobile Networks
    - Satellite Access Points
    - Cable Access Points
    - Wireline Access Points
    - Core Networking Systems
    - Long and Short Haul Networks
    - Storage and Cloud Based Services
    - End User and Edge Networking Equipment
    - Security and Operations

Contents

Figures

Tables

BACKGROUND

On May 15, 2019, the President signed Executive Order (EO) 13873: Securing the Information and Communications Technology and Services Supply Chain. This EO addresses the threat posed by the unrestricted acquisition or use of Information and Communications Technology (ICT) and services "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries," and declares a national emergency with respect to this threat.

The EO requires the Secretary of the Department of Homeland Security (DHS) to produce a written assessment within 80 days and annually thereafter that would "assess and identify entities, hardware, software, and services that present vulnerabilities in the United States and that pose the greatest potential consequences to the national security of the United States."[1] The assessment "shall include an evaluation of hardware, software, or services relied upon by multiple information and communications technology or service providers, including the communications services relied upon by critical infrastructure entities identified pursuant to Section 9 of Executive Order 13636."

Within DHS, the responsibility to execute the assessment was assigned to CISA/NRMC on behalf of the Secretary. In its response to this EO, the NRMC coordinated with federal and private partners to assess what ICT hardware, software, and services (referred to individually in this report as elements) present the greatest vulnerabilities in U.S. infrastructure and pose the greatest consequences.

SCOPE

Information technology and communications technology intersects almost every aspect of operations essential to national security, the Nation's critical infrastructure, and National Critical Functions (NCFs). NCFs are those functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof. DHS, through coordination with federal and industry partners, scoped its response to the Executive Order to accomplish the following:

- Develop a taxonomy of ICT elements based on Information Technology (IT) and Communication roles and sub-roles.[i]
- Assess the criticality of ICT element classes based on their sub-role and in the context of the IT or Communications sector function it supports.

This paper describes DHS's methodology for assessing ICT element criticality.

Caveats and Limitations

NRMC faced several challenges in responding to the EO including:

- Conducting a broad assessment with a short timeline that also allows a reasonable amount of time for vetting and validation with industry subject matter experts (SMEs), sector specific agencies (SSAs), and coordinating councils.
- Providing a general assessment of ICT element criticality independent from the application of the element in any specific network or system.[ii]
- Assessing an element known to support critical functions in some systems and non-critical functions in other contexts.

[i] In its response to the EO, DHS is assessing classes of elements rather than makes, models, and versions of elements, but will be able to use these assessments to assess specific makes, models, and versions within the most critical classes of elements in future iterations of analysis.

[ii] A system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- Identifying existing system-specific security measures that mitigate potentially risky attributes of technologies acquired through the supply chain.
- Handling technology trends geared to enable remote access, monitoring, administration, and control.

DHS will work to minimize and address these limitations as it develops its annual assessment as required by Executive Order 13873, as well as augment its assessments with additional analysis.

METHODOLOGY OVERVIEW

With support from Argonne National Laboratory and Sandia National Laboratories, DHS developed a two- step approach to assessing the criticality of ICT hardware, software, and services (ICT elements) in the IT and Communications sectors.[iii] In step 1, DHS developed an ICT Framework to decompose the basic roles and sub-roles ICT elements provide within the IT and Communications sectors, and then identified the elements that support each sub-role. In step 2, DHS developed and executed a repeatable approach for analyzing the criticality of ICT elements.

Each step of the methodology required extensive contributions from ICT SMEs. NRMC partnered with industry through a government established ICT Supply Chain Risk Management (SCRM) Task Force (ICT SCRM TF) to ensure the perspectives and expertise of critical infrastructure owners and operators could provide acute insight into operations and operational use of ICT. The ICT SCRM TF is a Critical Infrastructure Partnership Advisory Council (CIPAC) Cross Sector Working Group where the respective IT and Communications Sector Coordinating Council Chairs serve as the industry co-chairs. Accordingly, the co-chairs were able to solicit representative members from across the IT and Communications sectors, a majority of which are members of the Task Force, to provide input based on their experience and expertise. Additionally, the TF engaged non-member SMEs as necessary to provide inputs to inform the TF recommendations.

Step 1: Developing an ICT Framework

In step 1, DHS developed an ICT Framework to serve as a generic representation of IT and Communications sector roles and sub-roles, which would then be used to identify and bin ICT elements to draw basic judgements about criticality. The ICT Framework is organized into five roles (Local User Access, Transmission, Storage, Processing, and System Management) and 11 sub-roles, shown in figure 1 below.

To narrow the scope of the required EO assessment to a manageable, but meaningful initial response, DHS focused on the NCFs most closely aligned to the Communications sector and the portions of the Information Technology sector that the Communications sector depends on. These select NCFs, which align closely with the "Connect" theme, were chosen due to their extensive dependence on ICT elements, their criticality to other NCFs, and the criticality to national security of not just U.S. interconnectivity, but global interconnectivity. These NCFs enable all forms of communications in the United States, without which, all U.S. operations would be impacted with potentially catastrophic consequences:

- Operate Core Networks
- Provide Cable Access Network Services
- Provide Internet Routing, Access, and Connection Services
- Provide Radio Broadcast Access Network Services
- Provide Satellite Access Network Services
- Provide Wireless Access Network Services
- Provide Wireline Access Network Services

[iii] Due to time limitations, DHS was unable to analyze ICT elements for all critical infrastructure sectors. DHS chose to analyze the IT and Communications sectors because of their criticality for all other sectors.

These NCFs were selected due to their dependence on ICT elements and their criticality for other functions. See Appendix A for more information on NCFs.

When NCFs are decomposed into the ICT elements that support them, each element is organized into the ICT Framework (roles and sub-roles) shown below in figure 1:

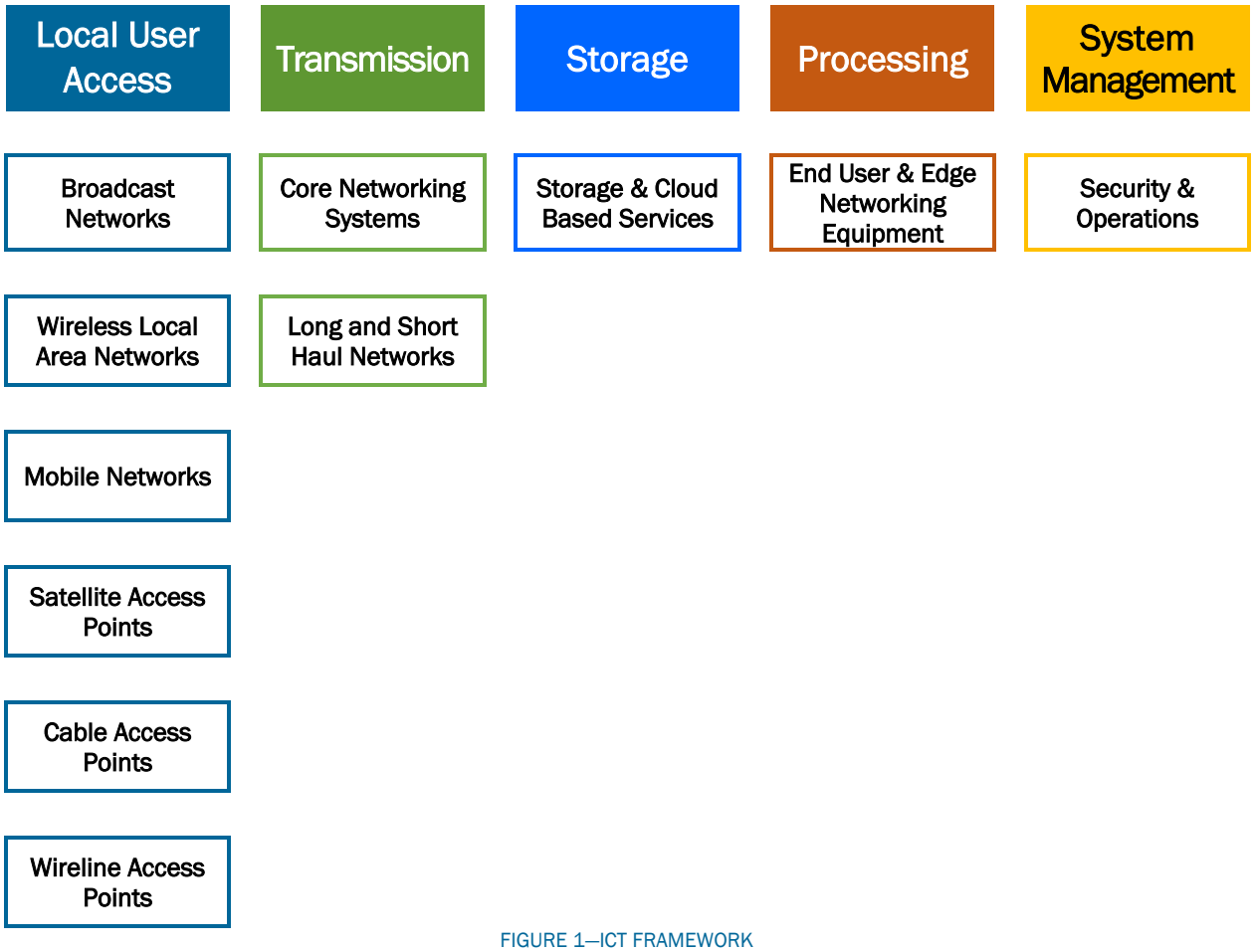


FIGURE 1—ICT FRAMEWORK

DHS identified 61 ICT elements (i.e. hardware, software, or services) that support 11 sub-roles of the ICT Framework. The list of 61 elements with definitions is below in table 1.

TABLE 1—ELEMENTS AND DEFINITIONS

ELEMENT	DEFINITION
BROADCAST NETWORKS	
Emergency Alert System (EAS) Encoder/Decoder	EAS encoder/decoders allow TV broadcast stations to take audio signals containing data and filter them for geographic region and emergency event information.
Station to Transmitter Link (STL)	The STL transports program material from a local station's studio to the station's transmitter site for broadcast.

ELEMENT	DEFINITION
Transmitter	A transmitter takes baseband audio, video, or digital signal and converts it to a radio frequency and amplifies it to drive a broadcast transmission antenna.
WIRELESS LOCAL AREA NETWORKS	
Distributed Antenna System (DAS)	A DAS is a network of spatially separated antennas that provide wireless service within a geographic area or structure. DAS will be applicable in Fifth Generation (5G); however, small cells and differing spectrum bands may change how a DAS is utilized.
Small Cells/Micro Cell	A small cell is a miniature base station that transmits short-range radio signals. Due to the limited range and non-penetrative signal of high frequency radio wave bands, 5G will require numerous small cells to support its infrastructure. Together, these cells would form a dense network that relays data through multiple small cells.
MOBILE NETWORKS	
Base Station Controller (BSC)	BSC controls facilitate communication between one or more base stations or cell sites.
Base Station Subsystem (BSS)	In a mobile cellular network, the BSS handles traffic between the cell phone and the network switching subsystem.
Base Transceiver Station (BTS)	A BTS is a 2G fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
Cell Session Control Function	A system that manages the signaling from end-user to services and other networks, providing the end-to-end connectivity across networks.
eNodeB	An eNodeB is a Fourth Generation (4G) Long-term Evolution (LTE) fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
gNodeB/5G NR	A gNodeB/5G NR is a 5G fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
NodeB	A NodeB is a 4G fixed communications location and is part of a network's wireless telephone system. It relays information to and from a transmitting or receiving unit, such as a mobile phone.
Home Agent	A router on a home network which enables communication to provider networks.

ELEMENT	DEFINITION
Home Location Register (HLR)	In a mobile cellular network, the HLR is the main database of permanent subscriber Personally Identifiable Information (PII) for a mobile network.
Home Subscriber Server (HSS)	The HSS is the master user database that supports the IP Multimedia Subsystem (IMS) network entities that handle calls and sessions. It contains user profiles, performs authentication and authorization of the user, and can provide information about the physical location of user.
Mobility Management Entity (MME)	The MME is responsible for idle mode user equipment tracking, paging procedure, activation and deactivation process, call handover, and user authentication.
Mobile Switching Center (MSC)	The MSC is the hub that handles many of the communication switching functions, including call setup, routing, release, messaging, and advanced features.
Equipment Identity Register (EIR)	The EIR is a database that contains a record of the all equipment that is allowed in a network and all equipment that is blacklisted.
Policy Decision Function	A ruleset engine that arbitrates the overall features and functions on the network that are available to users, and the allocation of resources and bandwidth available.
Mobile Positioning Center (MPC)	MPC is a service or function that that works to determine the position of a mobile device.
Gateway Mobile Location Center (GMLC)	GMLC is a service or function that that works to determine the position of a mobile device in mobile cellular networks. It is also expected to go away once there is a full conversion to 5G networks.
Media Gateway	A Media Gateway translates media content between various network and communication protocols.
Media Gateway Control Function (MGCF)	An MGCF performs switching and conversion between control switched and packet switched domains, connecting the mobile and standard telephony systems.
Gateway GPRS Support Node (GGSN)	A GGSN provides switching between the General Packet Radio Service (GPRS) network and packet switched networks, and routing on the GPRS mobile network.
Serving GPRS Support Node	A serving GPRS support node provides supporting functions for packet switched data within the network, such as user authentication and management.

ELEMENT	DEFINITION
Session Border Controller (SBC)	SBCs are used by all interconnected Voice over Internet Protocol (VoIP) providers and carriers to establish, maintain, and tear down phone calls through IP based networks.
Operation Support System (OSS)	OSS is comprised of hardware and software systems that allow network operators to perform network monitoring and management functions, such as configuration and provisioning. It also contains a large database of customer information and manages billing information.
SATELLITE ACCESS POINTS	
Satellite Payload	The space-based functional component of the communications platform. The satellite payload is the means by which the satellite mission is accomplished. Example satellite payloads include communications, PNT, signal detection, Overhead Persistent Infrared (OPIR), radar, imaging, etc. The payload may include some of the same component types as the satellite bus (e.g., communications transmitter/receiver, power amplifier, antenna, etc.) and often depends upon the satellite bus for a number of functions including power source, data processing, communication services, etc.
Satellite Bus	The space-craft system hosting the communications payload, which includes satellite navigation components, flight dynamics, fuel tank(s), thrusters, reaction wheels, solar panels, batteries, wiring harnesses, radiation shielding, the frame structures, power distribution, and a basic communication system for receiving instructions called TT&C (telemetry, tracking, and command). The satellite mission will determine the bus design or, conversely, the bus design will constrain the types of missions that can be supported by the satellite. For communications satellites, the payload may be integrated with the communications components of the satellite bus.
Satellite Ground Control Station (SGCS)	Facility providing satellite telemetry, tracking, and command (TT&C) connectivity from the Spacecraft Operations Center to the satellite.
Spacecraft Operations Center (SOC)	Terrestrial-based spacecraft operations facility that maintains the health and safety of the spacecraft and, if applicable, satellite mobility.
Communications Ground Station/Teleport	Ground equipment and facilities for managing subscribers, controlling subscriber access to services, providing billing for services, and providing interoperation between subscriber sessions and other networks.
Satellite Network Operations Center (SNOC)	Provides functionality to maintain network operations, such as providing user access, account management, and network health and operation.
Teleport Network	Terrestrial mesh of multi-terminal ground stations (Teleports) providing bulk space-ground connectivity, as well as interconnecting the various elements of Operations and Gateway Segments.

ELEMENT	DEFINITION
Uplink Facility	Terrestrial-based facility that provides uplink of content to be distributed to subscriber equipment.
CABLE ACCESS POINTS	
Core Server	A core server is a hardware and software system that provides functionality to other devices in the telecommunications backbone or core network, including data, processing, and management services.
Core Router	A core router directs packets through the network, specially designed for handling large volumes of data at high speeds as part of the telecommunications backbone.
Core Switch	A core switch performs packet switching operations, specially designed for handling large volumes of data at high speeds as part of the telecommunications backbone.
WIRELINE ACCESS POINTS	
Access Infrastructure Data Link	An access infrastructure data link is a communications pathway that provides data transmission services to wireline subscribers.
Access Infrastructure Digital Loop	An access infrastructure digital loop provides connectivity from the service provider to wireline subscribers.
CORE NETWORKING SYSTEMS	
Core Infrastructure SONET/SDH	Core Infrastructure SONET/SDH is a widely deployed technology used in implementing high-speed, large-scale Internet Protocol (IP) networks.
Core Infrastructure DWDM/OTN	Core Infrastructure DWDM/OTN are technologies that increase capacity on networks and optimize the existing resources of transportation networks.
Core Infrastructure IP/Internet	Core Infrastructure IP/Internet delivers data from the source host to the destination host within a communication network.
Core Infrastructure CDN Cache	A CDN is a system of distributed servers that deliver web pages and other content to users based on their geographic locations.

ELEMENT	DEFINITION
Core Infrastructure IP/MPLS	IP/Multiprotocol Label Switching (MPLS) refers to a network backbone that uses the IP augmented with MPLS routing. MPLS is a mechanism for routing traffic within a telecommunications network, as data travels from one network node to the next.
Data Center MPLS Routers	MPLS routers that support a data center.
Metro MPLS Routers	MPLS routers that support a metro area.
LONG AND SHORT HAUL NETWORKS	
Fiber Optic Cable	Fiber optic cable is the medium in which transmission of information as light pulses occurs along a glass, plastic strand, or fiber. Fiber optic cable is used across all domains (e.g., enterprise, long and short haul, cable, oceanic, etc.).
Repeaters	A repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than what would be capable with the original signal.
STORAGE AND CLOUD BASED SERVICES	
Server	A server is a hardware and software system that provides functionality to other devices in the system, including data, processing, and management services.
END USER EQUIPMENT & EDGE NETWORKING EQUIPMENT	
LAN Equipment (sensitive)[iv]	Local Area Network Equipment (sensitive) facilitates communication between one or more computers and other devices in a limited geographic area within a sensitive system. Typical equipment includes routers, switches, network interfaces cards, and cables.
LAN Equipment (non-sensitive)	Local Area Network Equipment (non-sensitive) facilitates communication between one or more computers and other devices in a limited geographic area that is not within a sensitive system. Typical equipment includes routers, switches, network interfaces cards, and cables.
Mobile Devices (sensitive)	Mobile devices (sensitive) are handheld, portable computing devices that can connect to a cellular network and process classified or sensitive information. Commonly refers to cellular phones, but can also refer to tablets, e-readers, and other devices that can connect to a cellular network.
Mobile Devices (non-sensitive)	Mobile devices (non-sensitive) are handheld, portable computing devices that can connect to a cellular network and process information that is not classified or sensitive. Commonly refers to cellular phones, but can also refer to tablets, e-readers, and other devices that can connect to a cellular network.

[iv] An element is designated as sensitive if it resides within a network or system that contains classified or sensitive data such that, if the data's confidentiality, integrity, or availability were to be compromised, there could be severe consequences. Examples of such networks include federal, military, and certain critical infrastructure networks.

ELEMENT	DEFINITION
Computers (sensitive)	Computers (sensitive) are general-purpose computers designed to be used by a single end-user (to include business staff one at a time) within a sensitive network or system, or process classified or sensitive data.
Computers (non-sensitive)	Computers (non-sensitive) are general-purpose computers designed to be used by a single end-user (to include business staff one at a time) and are not located within a sensitive network or system, nor process classified or sensitive data.
SECURITY & OPERATIONS	
Domain Name System (DNS)	DNS translates internet domains and hostnames to IP addresses.
Systems Software (sensitive)	Systems software (sensitive) includes the programs that are dedicated to managing the computer itself, such as the operating system, security software, and file management utilities, and have been installed on sensitive systems.
Systems Software (non–sensitive)	Systems software (non-sensitive) includes the programs that are dedicated to managing the computer itself, such as the operating system, security software, and file management utilities and have not been installed on a sensitive system.
Applications Software (sensitive)	Applications software (sensitive) includes software that enables the user to complete tasks, such as creating documents, spreadsheets, databases and publications, doing online research, sending email, designing graphics, and running businesses and has been installed on a sensitive system.
Applications Software (non–sensitive)	Application software (non-sensitive) includes software that enables the user to complete tasks, such as creating documents, spreadsheets, databases and publications, doing online research, sending email, designing graphics, and running businesses and is not installed on a sensitive system.

Step 2: Assessing Criticality

In step 2, DHS developed and executed a repeatable approach for assessing the criticality of ICT elements. DHS assessed the criticality of each ICT element in the context of the IT or Communications sector function it supports. This enabled DHS to distinguish the criticality of similar elements used in different sub-roles, for example, the difference in the criticality of routers used in core networks responsible for routing terabytes of data as opposed to routers used in home networks for personal use.

DHS worked with SMEs from CISA, industry partners, and national laboratories to collect data to analyze element criticality. Elements were assessed at the following criticality levels:[v]

- **Critical:** Compromise of the element could create an unacceptable amount of risk to the national security of the United States. There would likely be significant regional or national impacts, including

[v] DHS assessed the criticality of element classes based on how their compromise could affect the sub-role they support. With the exception of edge ICT elements (end user equipment, edge networking equipment, and end user software) which DHS assessed based on whether they were used in sensitive or non-sensitive networks, DHS did not identify specific elements that may be more or less critical based on what entities rely on them. For example, an element that supports military functions may be more critical than a similar element that does

affecting operations and the confidentiality, integrity, or availability of data or the system, and the ability to effectively mitigate these risks is uncertain or unsatisfactory.

- **Manageably Critical:**[vi] Compromise of the element could potentially have significant regional or national impacts, including affecting the confidentiality, integrity, or availability of data or the system, but risks can be mitigated with reliable and reasonable measures when properly implemented, such as using encryption or having redundant components supplied by multiple vendors and manufacturers.
- **Not Critical:** Compromise of the element is unlikely to have significant regional or national impacts.

DHS assessed the criticality of 61 ICT elements from the perspective of an administrator or network operator with privileged access. The ICT element criticality assessments can be analyzed collectively to prioritize supply chain risk management efforts.

DHS conducted and continues to refine its assessments[vii] of element criticality and risk. This analysis contains sensitive information and is not included in this public document.

IMPLICATIONS FOR THE FIFTH GENERATION (5G) NETWORK

5G, the next generation mobile network, represents a complete transformation of telecommunication networks. Combining new and legacy elements and infrastructure, 5G will build upon previous generations in an evolution that will occur over many years, utilizing existing infrastructure and technology. As 5G technologies are deployed, some elements may become more or less critical due to increasing or decreasing reliance upon them, or changes in how they are used. Distributed antenna systems will continue to be used in 5G, but the use of small cells[viii] and differing spectrum bands may change how a DAS is utilized. eNodeB/5G NR are 5G fixed communications locations that relay information to and from a transmitting or receiving unit, such as a mobile phone. eNodeB/5G performs a similar function as eNodeB (4G LTE) and NodeB (4G) elements, and as we move towards 5G, the criticality of elements from previous generations may require reassessment. GMLC are expected to go away completely once there is a full conversion to 5G networks. It is likely that 5G's development and deployment and other changes to the IT and Communications sectors will require the revaluation of some elements' criticality, and potentially the introduction of new elements to this assessment.

FUTURE ANALYSIS

DHS' initial analysis in response to Executive Order 13873 is foundational and will support future ICT supply chain analysis. Topics for future analysis may include:

- **Identify and Assess the Criticality of Elements in Other Sectors:** DHS will work with SMEs from other sectors and expand upon this analysis to identify and assess the ICT elements critical to those sectors.
- **Identify and Assess Specific Makes, Models, and Versions of Hardware, Software, and Services:** DHS' initial assessment and methodology may be used in follow-on analysis to identify elements of ICT hardware, software, and services, including analyzing specific products and services to understand the potential vulnerabilities they introduce and the potential consequences they pose.
- **Identify and Evaluate Entities that Manufacture or Provide Critical ICT Elements**: DHS may identify the key suppliers and manufacturers of critical ICT elements, and work with the Office of the Director of

not support military operations. Future analysis is planned to identify specific elements whose compromise would have potentially more significant consequences based on system deployment use cases.

[vi] Manageably Critical elements are still critical. There could still be significant national security consequences if key mitigations are not in place—such as vendor diversity, element redundancy, and encryption.

[vii] The list of ICT element criticality assessments, while "final," is not a permanent list, but will be dynamic and updated periodically to reflect current data on supply, demand, concentration of production, innovation in ICT sectors, new vulnerability considerations, and new mitigation considerations. This final list will serve as the Department of Commerce's initial focus as it develops its report to comply with Executive Order 13873.

[viii] Small cells and micro cells are miniature cellular towers that transmit short-range radio signals.

National Intelligence (ODNI) to incorporate threat analysis into its ICT supply chain analyses. Additionally, DHS reviewed the ODNI EO 13873 response before finalizing this report and found that the two products are complementary for meaningful subsequent analysis.

- **Identify the Most Critical Users of Critical ICT Elements:** DHS may identify entities within the United States whose use of compromised ICT Elements could result in the greatest consequences.
- **Identify or Assess Technology Serving Primarily Physical Purposes:** DHS may expand its list of elements to include Operations Technology (OT), such as programmable logical controllers (PLCs), and Internet of Things (IoT) technology, such as networked thermostats and telematics equipment, which serve primarily physical purposes.[ix]
- **Compare the Consequences of Data Theft with the Consequences of System Damage or Disruption:** It is likely that the set of entities identified as having high potential consequences from data theft will be different from the set of entities identified as having high potential consequences from damage or disruption.
- **Evaluate the Potential Impacts from Mitigation Activities:** DHS may evaluate the potential impacts to U.S. entities from various mitigation activities. This could include evaluating how identified threats might respond to mitigation actions taken by U.S. entities, including the Federal Government, and what the possible consequences of those responses would be for national security. DHS' written assessment may be used in follow-on analysis to analyze potential threat countermoves and their possible consequences.
- **Analyze ICT Elements Throughout the ICT Supply Chain Phases:** DHS may evaluate elements and assess risk throughout each phase of the supply chain:[2]
    - Phase 1: Design
    - Phase 2: Development and Production
    - Phase 3: Distribution
    - Phase 4: Acquisition and Deployment
    - Phase 5: Maintenance
    - Phase 6: Disposal

[ix] DHS defines IoT as "the connection of systems and devices with primarily physical purposes (e.g., sensing, heating and cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems."

APPENDIX A: NATIONAL CRITICAL FUNCTIONS

NCFs are those functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof. This assessment focuses on the *Connect* theme of the National Critical Functions list as it covers the backbone of national connectivity that enables cross-country and global operations. Please see table 2 below:

TABLE 2—NATIONAL CRITICAL FUNCTIONS

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
▪ Operate Core Network ▪ Provide Cable Access Network Services ▪ Provide Internet Based Content, Information, and Communication Services ▪ Provide Internet Routing, Access, and Connection Services ▪ Provide Positioning, Navigation, and Timing Services ▪ Provide Radio Broadcast Access Network Services ▪ Provide Satellite Access Network Services ▪ Provide Wireless Access Network Services ▪ Provide Wireline Access Network Services	▪ Distribute Electricity ▪ Maintain Supply Chains ▪ Transmit Electricity ▪ Transport Cargo and Passengers by Air ▪ Transport Cargo and Passengers by Rail ▪ Transport Cargo and Passengers by Road ▪ Transport Cargo and Passengers by Vessel ▪ Transport Materials by Pipeline ▪ Transport Passengers by Mass Transit	▪ Conduct Elections ▪ Develop and Maintain Public Works and Services ▪ Educate and Train ▪ Enforce Law ▪ Maintain Access to Medical Records ▪ Manage Hazardous Materials ▪ Manage Wastewater ▪ Operate Government ▪ Perform Cyber Incident Management Capabilities ▪ Prepare for and Manage Emergencies ▪ Preserve Constitutional Rights ▪ Protect Sensitive Information ▪ Provide and Maintain Infrastructure ▪ Provide Capital Markets and Investment Activities ▪ Provide Consumer and Commercial Banking Services ▪ Provide Funding and Liquidity Services ▪ Provide Identity Management and Associated Trust Support Services ▪ Provide Insurance Services ▪ Provide Medical Care ▪ Provide Payment, Clearing, and Settlement Services ▪ Provide Public Safety ▪ Provide Wholesale Funding ▪ Store Fuel and Maintain Reserves ▪ Support Community Health	▪ Exploration and Extraction of Fuels ▪ Fuel Refining and Processing Fuels ▪ Generate Electricity ▪ Manufacture Equipment ▪ Produce and Provide Agricultural Products and Services ▪ Produce and Provide Human and Animal Food Products and Services ▪ Produce Chemicals ▪ Provide Metals and Materials ▪ Provide Housing ▪ Provide Information Technology Products and Services ▪ Provide Materiel and Operational Support to Defense ▪ Research and Development ▪ Supply Water

National Critical Functions: The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

DHS' assessment specifically addresses the following National Critical Functions (NCFs) within the *Connect* theme:

- Operate Core Network
- Provide Cable Access Network Services
- Provide Internet Routing, Access, and Connection Services
- Provide Radio Broadcast Access Network Services
- Provide Satellite Access Network Services
- Provide Wireless Access Network Services
- Provide Wireline Access Network Services

To narrow the scope of the required EO assessment to a manageable, but meaningful initial response, DHS focused on the NCFs most closely aligned to the Communications sector and the portions of the Information Technology sector that the Communications sector depends on. The focus on NCFs within these sectors was due to the extensive dependence of these NCFs on ICT elements, their criticality to other NCFs, and the criticality to national security of not just U.S. interconnectivity, but global interconnectivity. These NCFs enable all forms of communications in the United States, without which, all U.S. operations would be impacted with potentially catastrophic consequences.

APPENDIX B: GLOSSARY

Broadcast Networks: Identified as a sub-role in the ICT Framework. Networks consisting of free and subscription-based, over-the-air radio and television (TV) stations that offer analog and digital audio and video programming services and data services.

Cable Access Points: Identified as a sub-role in the ICT Framework. Systems offering access to analog and digital video programming services, digital telephone service, and high-speed broadband services. Utilizes a mixture of fiber and coaxial cable commonly referred to as a hybrid fiber/coaxial (HFC) network to provide bi-directional signal paths to the customer.

***Connect* Theme (of National Critical Functions):** The NCF *Connect* theme contains nine critical functions, including: Operate Core Network; Provide Cable Access Network Services; Provide Internet Routing, Access, and Connection Services; Provide Radio Broadcast Access Network Services; Provide Position, Navigation, and Timing Services; Provide Internet-Based Content, Information, and Communication Services; Provide Satellite Access Network Services; Provide Wireless Access Network Services; and Provide Wireline Access Network Services.

Core Networking Systems: Identified as a sub-role in the ICT Framework. Core networking systems (also known as "backbone" systems when used to describe internet networks) facilitate the exchange of information among various sub-networks.

Critical: This is a criticality determination made by the National Risk Management Center. Compromise of the element could create an unacceptable amount of risk to the national security of the United States. There would likely be significant regional or national impacts, including affecting operations and the confidentiality, integrity, or availability of data or the system, and the ability to effectively mitigate these risks is uncertain or unsatisfactory.

Criticality Criteria: Criticality criteria considers important factors that will have the greatest impact on consequences.

End User Equipment and Edge Networking Equipment: Identified as a sub-role in the ICT Framework. End user equipment is any device used by an end-user to communicate, while edge networking equipment provide an entry point for end user equipment to connect into core networking systems. Examples include cellular phones, desktop and laptop computers, and tablets; related local area network infrastructure; and related software.

ICT Element: An ICT element is a type of hardware, software, or service.

ICT Element Core Factors: Core factors are the low-level functional operations performed by individual ICT elements that collectively contribute to determining overall criticality of the element.

ICT Framework: The ICT Framework is comprised of generic representation of ICT systems, which will serve as an organizing principle for binning ICT elements and drawing basic judgements about criticality.

Independent Mitigation: Non-element functions obviate concerns. This is one criticality criterion used by the National Risk Management Center to make criticality determinations.

Local User Access: One of five determined ICT Framework roles. Systems facilitating individual or group user access, via devices, to telecommunications and internet resources.

Long Haul and Short Haul Networks: Identified as a sub-role in the ICT Framework. Communication networks spanning both long and short distances.

Manageably Critical: This is a criticality determination made by the National Risk Management Center. Compromise of the element could potentially have significant regional or national impacts, including affecting

the confidentiality, integrity, or availability of data or the system, but risks can be mitigated with reliable and reasonable measures when properly implemented, such as using encryption or having redundant components supplied by multiple vendors and manufacturers.

Mobile Networks: Identified as a sub-role in the ICT Framework. Also known as "cellular networks." A communication network where the last link is wireless. The network is distributed over land areas called cells, each served by at least one fixed-location transceiver. When joined together, these cells provide radio coverage over a wide geographic area.

National Critical Functions (NCFs): NCFs are those functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof.

Not Critical: This is a criticality determination made by the National Risk Management Center. Compromise of the element is unlikely to have significant regional or national impacts.

Processing: One of five determined ICT Framework roles. Systems supporting the creation and manipulation of data or information for a variety of purposes.

Roles: Roles are represented as the five top-level headings of the ICT Element Framework (local user access, transmission, storage, processing, and system management). ICT roles group ICT elements into broad categories of ICT operations they facilitate.

Satellite Access Points: Identified as a sub-role in the ICT Framework. Systems offering access to platforms launched into orbit to relay voice, video, or data signals as part of a telecommunications network.

Security and Operations: Identified as a sub-role in the ICT Framework. Devices, services, and software that provide security and operational functions within a network.

Security Features: Hardware, software, and services that are integrated into ICT systems to provide protection from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide (i.e., anti-virus/anti-malware, IDS/IPS, encryption, authentication, etc.).

Sensitive: An element is designated as sensitive if it resides within a network or system that contains classified or sensitive data such that, if the data's confidentiality, integrity, or availability were to be compromised, there could be severe consequences. Examples of such networks include federal, military, and certain critical infrastructure networks.

Sub-Roles: Sub-Roles further group ICT elements into narrower operational roles under each of the five ICT roles. ICT elements are decomposed under the sub-roles they support.

Storage: One of five determined ICT Framework roles. Systems supporting retention of data generated by computers and other devices generated either locally or remotely.

Storage and Cloud Based Delivery: Identified as a sub-role in the ICT Framework. Computer data storage and delivery, either on a local server, or (in the case of cloud-based) on multiple servers across multiple locations.

System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.[3]

System Management: One of five determined ICT Framework roles. Devices, services, and software serving functions required for system operation, security, and maintenance.

Transmission: One of five determined ICT Framework roles. Systems supporting the process of sending data over a communication medium to one or more computing, network, transit network, communication or electronic devices in a point-to-point, point-to-multipoint, or multipoint-to-multipoint environment.

Wireless Local Area Networks: Identified as a sub-role in the ICT Framework. Systems offering access to telecommunication in which electromagnetic waves (rather than wire) carry the signal over part of or the entire communication path.[x]

Wireline Access Points: Identified as a sub-role in the ICT Framework. Circuit- and packet-switched networks via copper, fiber, and coaxial transport media.

[x] Wireless technologies consist of cellular phones, wireless hot spots (WiFi), personal communication services, high-frequency radio, unlicensed wireless, and other commercial and private radio services to provide communication services.

[1] President of the United States. Executive Order 13873—Securing the Information and Communications Technology and Services Supply Chain. May 15, 2019. https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain. Accessed on January 16, 2020.
[2] DHS/CISA/NRMC. December 2018. Supply Chain Risks for Information and Communication Technology. https://www.cisa.gov/sites/default/files/publications/19_0424_cisa_nrmc_supply-chain-risks-for-information-and-communication-technology.pdf. Accessed on January 16, 2020.
[3] NIST. Computer Security Resource Center. "System." 2019. https://csrc.nist.gov/glossary/term/system. Accessed on January 16, 2020.

DHS POINT OF CONTACT

National Risk Management Center
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
NRMC@cisa.dhs.gov
For more information about NRMC, visit www.cisa.gov/national-risk-management.
PDM19058

Appendix 5

Summary of Responses to the NTIA Secure 5G Request for Comment, July 27, 2020

Summary of Responses to the NTIA Secure 5G Request for Comment

Introduction

In accordance with the Secure 5G and Beyond Act of 2020,[1] on May 28th, 2020 the National Telecommunications and Information Administration (NTIA) published a Request for Comment (RFC)[2] to inform the development of an Implementation Plan for the National Strategy to Secure 5G (Strategy).[3] NTIA received more than 70 comments from a range of stakeholders, including industry associations from multiple sectors of the 5G ecosystem, companies, think tanks, and individuals.

This report represents a high-level summary of the RFC responses to inform the Implementation Plan developed by the National Security Council and the interagency.

Key Themes

This section describes key themes NTIA extracted from the RFC responses to inform the development of the Implementation Plan. These themes have been organized by the lines of effort identified by the Strategy. For this summary, NTIA focused on the RFC responses that provided information relevant to the implementation of the National Strategy to Secure 5G. Not all subjects raised by respondents are summarized here.

Each theme includes a summary statement highlighting respondents' viewpoints. NTIA has included excerpted quotes from various RFC responses to illustrate these viewpoints. These excerpts are representative only; they are not intended to be exhaustive of all the responses received on that theme.

Please note: RFC response excerpts are not edited for spelling, grammar, punctuation, or typographical errors. References have been removed. All comments can be found at: https://www.ntia.doc.gov/federal-register-notice/2020/comments-national-strategy-secure-5g-implementation-plan.

[1] Secure 5G and Beyond Act of 2020, Pub L. No. 116-129, 134 Stat. 223-227 (2020) (Act).
[2] The full request for comment can be found at https://www.ntia.doc.gov/federal-register-notice/2020/request-comments-national-strategy-secure-5g-implementation-plan.
[3] *See*, The National Strategy to Secure 5G of the United States of America, March 2020, *available at* https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

Line of Effort 1: Facilitate Domestic 5G Rollout

Theme: Spectrum

Summary: The most discussed theme with regards to the facilitation of domestic 5G development was the need to make more spectrum available for commercial use. While many commenters focused on mid-band allocation, many called as well for both high- and low-band spectrum to be released for commercial use. Commenters also noted the importance of promoting spectrum sharing as a means to maximize the use of limited spectrum resources.

RFC Response Examples:

- **National Spectrum Consortium [p. 9]:** Spectrum sharing is another area in which research should focus on dual-purpose technologies that will satisfy both government and commercial users. Spectrum sharing is a critical policy and technology solution that ensures that access to the limited spectral resource does not need to be a zero sum game. Through spectrum sharing technology, government and commercial users can share spectrum resources, protecting mission critical operations and making spectrum available to other users when and where the spectrum is available.
- **Verizon [p. 3]:** As the Administration and the FCC are well aware, however, large, contiguous blocks of mid-band spectrum, made available for licensed, flexible-use service, will be critical for U.S. leadership in 5G.
- **ACT The App Association [p. 3]:** The Strategy should set the identification of new opportunities for reallocation and/or new sharing arrangements across spectrum bands consistent with interference protection principles, including for government-owned spectrum bands that may be ideal for commercial IoT use, particularly mid-band and millimeter wave bands.
- **Alion Science and Technology [p. 2]:** Promote spectrum sharing by allowing shared use between Federal and non-Federal operations. For example, Department of Defense (DoD) could implement 5G technologies for use on DoD facilities or in the battlefield that would switch to wireless providers outside those areas. This would allow commercial industry to benefit from 5G research performed by the national and DoD Labs, as well as allow the Government to benefit from reduced costs by purchasing COTS equipment.

- **AT&T Services, Inc. [p. 3]:** Regarding spectrum policy, government should continue efforts to free up radiofrequency spectrum for 5G, and in particular spectrum (between 3 GHz and 8 GHz), particularly in the 3.1- 3.55 GHz range. Mid-band spectrum is particularly important for 5G because it offers a balance between wide geographic coverage and greater capacity and speed.
- **CTIA [p. 6]:** Leading the 5G economy will require a steady pipeline of spectrum auctions and continued modernization of infrastructure siting rules. These are the pillars of wireless regulatory policy that will drive continued deployment and innovation in 5G.
- **Samsung Electronics America [p. 4]:** U.S. competitiveness in 5G requires a combination of low, mid and high band spectrum. The Federal Communications Commission (FCC) made the U.S. a world leader in commercialization of high-band and low-band spectrum, in which carriers are deploying 5G. The FCC is now making crucially important progress on mid-band spectrum. The FCC should complete its scheduled CBRS and C-band auctions in a timely manner and proceed with additional mid-band spectrum allocations.
- **Competitive Carriers Association [p. 4]:** Spectrum is the lifeblood of the wireless industry. Nationwide wireless broadband and 5G deployment is contingent on the ability of all carriers to access a robust portfolio of spectrum resources. Competitive carriers must have access to a variety of low-, mid-, and high-band spectrum to meet consumers' insatiable demand for data. NTIA can enable advanced networks by including in its Implementation Plan steps to freeing up additional spectrum for wireless use in low-, mid-, and high-band frequencies.
- **Ligado Networks LLC [p. 2]:** The advancement to 5G promises to be transformative, but it will also require an extraordinary amount of spectrum, both in terms of total MHz and in terms of variety of bands. Spectrum best suited for wireless network deployments generally falls into four categories: (1) low-band (below 1 GHz); (2) lower mid-band (1-2 GHz); (3) higher mid-band (2-6 GHz); and (4) high-band spectrum (above 6 GHz and mmWave). 5G networks will need the right mix of spectrum from all four of these categories to succeed, and mid-band spectrum is a critical element that needs attention now.
- **USTelecom [p. 2]:** While enlightened spectrum policy is certainly necessary for successful 5G deployment, it is only one piece of the puzzle. Fiber backhaul facilities are just as important.

Theme: Regulatory Relief

Summary: Commenters commended the Administration's light-touch approach to regulation, and recommended that this be applied to the roll-out of 5G. Specifically, several commenters noted difficulties in siting and permitting, suggesting that this would in many cases require coordination with state and local officials.

RFC Response Examples:

- **Crown Castle [p. 3]:** Crown Castle urges the adoption of federal legislation providing regulatory relief nationwide through streamlining the permitting and regulatory processes for telecommunications infrastructure and equipment to promote broadband deployment, job creation and investment in next generation infrastructure.
- **Cisco [p. 5]:** The Administration Should Advance a Light Touch Regulatory Framework that Streamlines Deployment and Encourages Open and Interoperable Technology
- **Hughes Network Systems, LLC, EchoStar Satellite Services, L.L.C. [p. 4]:** In addition, in order to continue to lead in 5G and beyond, the U.S. government must also take action to

relieve unnecessary and burdensome regulations. To encourage U.S. based operators to launch and operate U.S. satellites and use the United States as a licensing administration and not the International Telecommunications Union as the filing administration, it is important that the Federal Communications Commission (FCC) address several areas where U.S. regulation is excessively burdensome. These areas include excessive bond requirements, "Three Strikes Your Out" Rules, and lack of flexibility in fleet management. All of these areas are even more burdensome when compared to other space faring nations that the United States competes with.

- **Nokia [p. 7]:** The current Administration's commitment to light-touch regulation of broadband has fueled continued investment in U.S. networks and continuation of that policy is critical to the U.S. keeping pace as the global leader in wireless technologies. Mobile operators will invest in critical capacity and capability, but are discouraged from doing so when the return on that capital deployed into infrastructure does not recover the cost.
- **Partnership for Interoperable Networks [p. 5]:** Identify existing regulation that impedes the operator procurement or deployment of interoperable or virtualized network equipment. Conduct a cost-benefit analysis of these regulations, including the benefits outlined in this paper, and where necessary update or remove them.

Theme: Procurement

Summary: Respondent comments on the suggested outcomes were generally positive, although some took issue with particular details or recommended adding others.

RFC Response Examples:

- **Mavenir Systems, Inc [p. 5]:** The U.S. is a purchaser of radios and private wireless networks domestically for its federal offices and military installations and abroad for its military bases and embassies. Accordingly, the U.S. should create volume-based government procurement opportunities to ensure national security and in volumes large enough to leverage its purchasing power to create scale for Open RAN solutions.
- **Open RAN Policy Coalition [p. 13]:** In particular, the Secretary of Defense should direct pertinent DoD personnel to (1) incorporate open and interoperable RAN in some portions of its future 5G programs both stateside and abroad (e.g., use a portion of its authorization to spend up to $275 million on Next Generation Information Communications Technology such as 5G to deploy interoperable network technology in connection with implementation of Section 226 of the FY2020 National Defense Authorization Act); (2) accelerate DoD programs, such as future National Spectrum Consortium 5G testbeds, to ensure open RAN solutions are incorporated in the FY2020 and FY2021 time periods; and (3) use DoD procurement authority to test and/or deploy 5G open and interoperable interface-based networks through the 5G to NextG solicitation (6-12 months out).
- **ARM [p. 3]:** To the questions of vendor diversity, 5G brings the prospect of wider use of 'virtualization' that is using software-based networks. This introduces the possibility of a RAN operating through software sitting on top of basic core equipment. There is very interesting and promising work occurring around this in bodies like 3GPP, O-RAN Alliance, and the Telecom Infra Project. The government should support these efforts, while also recognizing the important role traditional mobile network equipment companies will play in 5G deployment. To do this, it is important to enact policies that promote innovation and experimentation, but do not mandate specific technologies. For example, the government should…utilize government procurement as a means to support vendor diversity.

- **Aviat [p. 3]:** Many federal agencies have existing legal and procurement authorities to support private sector research and development work for agencies' procurement and adoption of mission-critical technologies like 5G. By investing R&D funds through contracts or other instruments (e.g. Other Transaction Authority agreements), the Government can incentivize Aviat Networks further investment in 5G by providing seed funding for prototype projects, and help reduce barriers that agencies have to confront in purchasing private sector developed cutting edge solutions.

Theme: Technologically Neutral Policy

Summary: Respondents were broadly supportive of policy that is technology neutral, e.g. policy that does not favor or specify a single technology over others when setting rules, regulations, or policies in which more than one technology could fulfill the stated policy goal.

RFC Response Examples:

- **Juniper Networks [p. 3]:** The government can overcome macro network barriers during the procurement process by the specification of open standards and open interfaces. This will increase competition, encourage innovation, and open the 5G market to new market entrants. Moreover, agencies that take advantage of competition and conduct market research that is open, transparent and brand neutral will better position themselves to build the most innovative and secure networks.
- **Satellite Industry Association [p. 2]:** SIA urges NTIA as it considers the best way to improve U.S. leadership in 5G and beyond to adhere to certain basic principles that have successfully guided the United States in the past. This includes utilizing a technology neutral approach in developing regulation including for the allocation of scarce resources such as spectrum and funding.
- **IBM [p. 5]:** While 5G entails similar kinds of telecommunications infrastructure as prior generations of wireless technology, it also includes an unprecedented amount of software and is much more reliant on newer technologies like cloud computing to manage network functions. As such, the line between the infrastructure layer and application layer in 5G is blurred. Industry and government in the United States and abroad should agree on a common model that clearly defines what 5G infrastructure entails and use existing global standards to evaluate and develop secure 5G infrastructure.
- **CTIA [p. 49]:** As discussed, O-RAN is a promising option, which offers disaggregated functionality built using open interface specifications between elements. The benefits of this type of development are based in vendor-neutral hardware and software-defined technology built through open interfaces and community-developed standards. According to the O-RAN Alliance, this will allow smaller vendors to introduce their own services and allow operators to customize the network as needed. It will also allow multiple vendors to deploy their technology on the network, thereby enabling competition and reducing costs. Open Core has also been getting attention as a way to innovate, including by the Telecom Infra Project. CSRIC VII, WG 2 addressed these, and other ongoing CSRIC workstreams are engaged as well.
- **Starry, Inc. [p. 6]:** To facilitate a robust 5G ecosystem, policymakers should avoid initiatives that favor one technology over another or impose regulatory burdens that would stunt innovation and investment. It should consider robust platforms for security that span technologies and standards, instead of ones tailored to specific technology implementations.

Theme: Funding

Summary: Commenters emphasized that government funding will play a large part in many aspects of 5G development. Some argued that through strategic grants, tax breaks, and other spending, the U.S. government can aid in many different 5G development efforts.

Sub-Theme: Rip and Replace

Summary: Replacing existing infrastructure is an expensive process that will require sufficient funding to be successful. Specifically commenters request that these efforts be aided through funding of "covered equipment and services" under Section 4 of the Secure and Trusted Communications Networks Act.[4] In addition, commenters requested that the FCC work to identify what needs to be replaced.

RFC Response Examples:

- **Competitive Carriers Association [p. 5]:** Securing the nation's 5G networks is of the utmost importance, but this worthy goal can only be achieved fully if sufficient funding is made timely available to those entities that must remove and replace equipment. The changes to the network can only be made if sufficient funding is available for this expansive process.
- **NEC Corporation of America [p. 5]:** Specifically, these efforts could be aided through funding the replacement of "covered equipment and services" under Section 4 of the Secure and Trusted Communications Networks Act. Some portion of this funding could be reserved for recipients who elect to use the funding to deploy network equipment which includes open interface standards-based compatible, interoperable equipment, such as equipment developed pursuant to the standards set forth by organizations such as the O-RAN Alliance and the Telecom Infra Project.
- **Open RAN Policy Coalition [p. 11]:** As we recommended to the Federal Communications Commission (FCC) in its ongoing proceeding to identify and replace "covered communications equipment and services," we believe the Administration should "further[] the flexibility and innovation that has yielded a diverse array of suppliers, a wide range of vibrant services, and enormous technological strides."

Sub-Theme: Research and Development

Summary: Commenters emphasized the need for funding for Research and Development. Many requested a federal grant program to create a system of standards to be used across 5G development. For 5G to be successful, some argued that new semiconductor technology needs to be developed and new manufacturing facilities need to be built. It was suggested that the U.S. government could provide funding for research and tax breaks for new facilities to help address these needs.

RFC Response Examples:

- **Semiconductor Industry Association [p. 2]:** A new federal grant program that would provide grants for incentivizing new domestic semiconductor manufacturing facilities (fabrication, assembly, test and advanced development) that align with our nation's strategic priorities. These federal grants would be in addition to state-level incentives.

[4] Secure and Trusted Communications Network Act of 2019, H.R. 4998, 116th Cong. § 4 (2019).

- **Partnership for Interoperable Networks [p. 4]:** Provide tax incentives for the procurement of interoperable infrastructure in public mobile networks. Approaches might include:
    - Tax relief for operators against the cost of procuring network infrastructure.
    - A sales tax exemption on the purchase of equipment and technologies that adhere to relevant international standards.

  Provide tax incentives against the cost of procuring interoperable network infrastructure for use in enterprise networks. Applicable use cases may include smart manufacturing and precision agriculture.
- **Alliance for Telecommunications Industry Solutions [p. 7]:** ATIS urges the U.S. Government to clarify that R&D tax credits apply to the development of next generation standards and the assessment of future technologies and architectures. Further, a special classification of R&D tax credits should be considered that is associated with a national set of 5G and beyond objectives, as defined by government and industry, which will further incentivize the private sector to promote U.S. leadership and contribute to the development of a core set of technologies that can drive the U.S. market.
- **Red Hat Inc. [p. 4]**: Accelerate research and development of open 5G technologies by industry, research agencies, and academia. This could include direct financial incentives for organizations leading these efforts; tax incentives, such as an increase in the R&D tax credit specifically for 5G investments; and investments in human capital, such as working with the National Science Foundation to spur R&D and skills development. This could also include an emphasis on open interfaces in federal research agencies and incorporate the use of open interfaces in 5G pilot projects.

Sub-Theme: Workforce Development

Summary: Respondents noted that funding is needed to train and deploy the large workforce that will be needed to install the infrastructure for 5G. With thousands of new jobs needing to be filled, education and training is essential to an effective roll out. Commenters stated that the federal government can coordinate with states to provide funding to educational programs as needed. Grants from the Department of Labor's Employment and Training Administration could be a key mechanism for properly funding workforce development.

RFC Response Examples:

- **Computing Technology Industry Association [p. 16]:** Estimates suggest that 20,000 job openings for tower climbers and telecommunications technicians must be filled in order to complete the country's 5G build. In Congress, bipartisan bills have been introduced in both the House and Senate to draw greater attention to these issues, and the Senate Commerce Committee held a hearing on this theme in early 2020. The Administration should support these and other efforts to ensure that worker shortages do not slow down 5G deployment at a moment when other countries are also pushing to deploy networks rapidly.
- **Ericsson [p. 12]:** To implement the National Strategy to Secure 5G, Ericsson urges the federal government to collaborate with state and local governments and industry partners to develop the workforce. Vocational education awareness (state and local level): State education boards should emphasize the option of 5G vocational skills earlier in the U.S. education cycle. State education boards should work with industry participants to create standardized curriculums around 5G vocational skills. At the federal level, the TOWER Infrastructure Deployment Act (H.R. 3255) would direct the FCC to address this issue and

develop recommendations for Congress on ways to encourage a larger 5G workforce. Congress should pass this bill to expedite efforts to increase the 5G workforce in the U.S.

- **Fiber Broadband Association [p. 17]:** Federally-supported workforce development programs further provide productive opportunities to support and expand educational opportunities. The Department of Labor ("DOL") Employment and Training Administration oversees two grant programs that can make a difference. FBA has called on DOL to prioritize granting funds for broadband deployment, fiber deployment, and 5G training – calling out those areas in their grant programs and announcements specifically.
- **Wireless Infrastructure Association [p. 7]:** A persistent barrier to 5G deployment is an understaffed wireless workforce. It is estimated that the industry needs to train 20,000 more tower climbers to install the equipment necessary to enable 5G. That number balloons to an estimated 100,000 more workers when accounting for critical jobs like radiofrequency (RF) engineers, site surveyors, and radio tuners. The reality is that China can more quickly to deploy labor at lower costs. If the U.S. wants to remain competitive in the race to 5G, the Federal Government must invest in programs that will train this critical workforce. The Department of Labor has already been a great ally of the wireless workforce, but more work remains to be done. By investing in programs like TIRAP, the Administration can empower individuals and bring quality jobs to communities that are not contingent on costly four-year degrees.

Line of Effort 2: Risks to & Identify Core Security Principles of 5G Infrastructure

Theme: Risk-Based Approach

Summary: When identifying potential security vulnerabilities, commenters emphasized a risk based approach, specifically in the supply chain of infrastructure components. They argued that the U.S. government should collaborate with supply chain stakeholders to have transparency where risks lie, and that a singular focus on equipment would stifle what should be a national focus on holistic security. Some posited that the U.S. government should not outright ban foreign suppliers, but instead evaluate risks and make evidence based decisions.

RFC Response Examples:

- **Hewlett Packard Enterprise [p. 5]:** Component and sub-component supply chains that are not in the U.S. may pose a known but unaddressed source of compromised 5G infrastructure. Risks need to be addressed in priority order based on threat of compromise. Industry and government should work together to identify and analyze the risks in components and sub-components, including printed circuit board manufacturing, complex cable assemblies such as iSCSI, Ethernet, InfiniBand and others, logic bearing sub-components with internal bus connectivity to the platform such as CAN/MIC bus or other unprotected busses, or internet connectivity.
- **Information Technology Industry Council [p. 2]:** We recommend that policymakers take a risk-based approach to 5G security, ensuring that any effort is evidence-based and fit-for-purpose. Policymakers should consider how to address the full range of risks as a singular focus on equipment and suppliers threatens to stifle what should be strong national attention on the full breadth of 5G security issues.

- **Juniper Networks [p. 3]:** Juniper recommends that NTIA, as it is doing now, work collaboratively with stakeholders to assess risk and identify security principles that are core to 5G infrastructure. NTIA has a well-regarded track record of convening parties on all sides of issues to analyze complex issues and arrive at consensus decisions. The assessment of risk and identification of principles are no different.
- **Xcom Labs [p. 2]:** The government should use a risk-based approach and not outright ban infrastructure components from other countries. Critical software and hardware should be developed by US vendors when possible, but the hardware often can be safely manufactured/sourced from outside of the U.S. There should be a clearly outlined process to validate certain vendor components for core network (EPC, NGC), network management functions, centralized units (CU), distributed units (DU), switches and gateways, as well as associated chipsets from any country.
- **Booz Allen Hamilton [p. 13]:** FirstNet should engage its stakeholders and standards bodies (e.g., NIST) to develop and prioritize security requirements for various user groups, applications, and operational situations. Working with these groups and service providers, FirstNet should also conduct a thorough risk analysis to identify threats and vulnerabilities to the various system elements (e.g., networks, devices, applications). FNN solutions will need to address these risks, as well as specific challenges—such as achieving interoperability among agencies with different security policies and ensuring minimum security requirements across interconnected systems— associated with a network involving multiple agencies, jurisdictions, and owners. FirstNet should also develop comprehensive security plans that define how security solutions will be implemented and maintained by FNN solution provider(s), and tested, certified and monitored by the cognizant government authority.

Theme: Zero-Trust Architecture

Summary: Many commenters emphasized the need for a zero-trust architecture in 5G deployment. Further, respondents noted that having a data-centric architecture would improve the overall security of the network and verifying all components of the network allows for better access control and makes breaches easier to detect. They stated that the U.S. government could advance zero-trust by developing standards and best practices through NIST.

RFC Response Examples:

- **BSA The Software Alliance [p. 3]:** Ultimately, securing the 5G ecosystem may be best approached by applying "zero trust" principles. Zero trust architectures assume that all users and data within a network could be a threat and build flexible layers of protections to mitigate those threats, ranging from supply chain disruptions to insider attacks. Building zero trust 5G environments requires decoupling hardware and software systems wherever possible, robust user authentication protocols, ubiquitous encryption, and a strong open source-driven architecture. The Administration can advance zero trust approaches through contributing to standards development, best practice guidance, and R&D. Piloting zero trust approaches to 5G security, as NIST is currently preparing to do, is an important priority in this area.
- **Dell Technologies [p. 5]:** Zero trust or data-centric architectures put forth basic tenets or principles to secure modern infrastructure against today's threat landscape in which the primary concern is nation state sponsored threat actors. These tenets apply not only to core infrastructure, cloud, and edge, but also to the span of 5G technologies. The current threat landscape consists of sophisticated threat actors who will find the weak point in any system or within the ecosystem of the supply chain or connected devices. If a vulnerability exists, it

will be identified, cataloged and used for exploits by a threat actor. As such, the principles of the zero trust architectural model build in safeguards to prevent an attacker from moving beyond their initial foothold, make it more difficult for an attacker to maintain that initial foothold, while enabling detection early in the Kill Chain to minimize the amount of time an attacker remains on the network (dwell time).

- **Oracle [p. 4]:** 5G's transition from purpose-built hardware to software and cloud presents a new opportunity to shift the security advantage. Built in the cloud, 5G inherits the cloud's scale, reliability and security, allowing capabilities to be rapidly deployed, scaled, and segmented with tailored security measures applied to each. Embedded artificial intelligence and machine learning capabilities can autonomously prevent, detect, respond to, and predict sophisticated threats. As the network functions are carried out in software, there are additional tools such as network slicing, containerization, and zero-trust software defined perimeters to further enhance security.
- **National Spectrum Consortium [p. 9]:** NSC and its members are working at the leading edge of zero trust, setting up reference architectures and requiring that each 5G testbed run by NSC members include implementation of zero trust security. The Administration's Implementation Plan should require commercial industry to work with the U.S. Government on zero trust architectures that will enable deployment of zero trust technology in each private, public and government 5G implementation. The Administration also should think beyond 5G and consider security approaches for future wireless technologies that are still in very early stages of development, in order to build security into the technologies and standards from the start.
- **Q Networks LLC [p. 2]:** The U.S. Government would be prudent to only do business and operate with vendors that support counterintelligence programs, principles of nuclear surety, and zero trust security best practices and it must ensure that all existing and pending technology contracts are aligned with a secure, American-sourced 5G network enablement strategy. These initiatives, specifically, are critical when evaluating security gaps in 5G infrastructure. Furthermore, stakeholder-driven approaches that the U.S. Government should mandate in all government technology contracts include zero trust security and American-sourced end-to-end solutions.

Theme: Harmonization of Federal Efforts

Summary: The U.S. government needs to work towards harmonization of federal efforts. Rollout of 5G will be slowed by fragmented efforts by different areas of the government in forming security and supply chain policies. Overlapping governance can cause confusion and unnecessary roadblocks. The U.S. government should form a coherent strategy with all public and private stakeholders.

RFC Response Examples:

- **ADTRAN Inc. [p. 9]:** The 5G Implementation Plan Notice seeks comment on the factors the government should consider in developing core security principles for 5G deployment, and on the factors the government should consider in evaluating potential security gaps. As an initial matter, ADTRAN believes that there should be harmonious treatment of these national security issues across the federal government, as well as in undertakings to partner with the private sector in ensuring that 5G networks in the United States will be secure. There are efforts underway to coordinate the Executive agencies' 5G national security activities under the auspices of the Department of Commerce. The Federal Communications Commission is

separately addressing the exclusion of equipment that presents national security risks from the Universal Service Fund subsidy program. In addition, the federal government is working with the private sector to address ICT supply chain security, which would include 5G.

- **CTIA [p. 31]:** One underdeveloped area in the National Strategy to Secure 5G is the harmonization of existing federal work on 5G security. There are many fragmented efforts underway, so NTIA should encourage harmonization to avoid conflicting or overlapping work.
- **BSA The Software Alliance [p. 5]:** As 5G becomes increasingly critical across numerous sectors, there is a risk of incoherent and overlapping governance. 5G will be a critical technology in the communications sector, the transportation sector (where 5G will enable broader adoption of autonomous vehicles), the health care sector (where 5G will support life-critical medical devices), the financial sector (where 5G will underpin online financial transactions), and others. Whereas previous generations of communications networks could be regulated strictly as telecommunications services, 5G depends on core infrastructure – such as cloud services – that simultaneously serves multiple functions and clients, making it a poor fit for telecommunications-specific regulations. Successful governance will require a unified approach across sectors and agencies. Such governance mechanisms must be flexible and build risk-based approaches that tailor compliance requirements to each 5G network's specific uses and threats. Multiple agencies across the U.S. government have already begun to adopt 5G policies; the Administration should act now to establish effective mechanisms to enforce coordination and coherence across agencies.
- **Cubic Nuvotronics [p. 2]:** Collaboratively consolidate research initiatives across DARPA, Intelligence Advanced Research Projects Activity (IARPA), National Laboratories, Service Laboratories, Federally Funded Research and Development Centers/University Affiliated Research Centers (FFRDCs/UARCs) for focus and impact. Consolidate test beds where possible and externalize their use.

Theme: Public-Private Partnerships

Summary: Commenters called for the U.S. government to continue to work closely with the private sector, and to focus on public-private partnerships in the development of a secure 5G ecosystem.

RFC Response Examples:

- **NTCA – The Rural Broadband Association [p. 9]:** NTCA encourages NTIA and other federal agencies to engage in ongoing coordination of cyber security principles and guidelines. Such coordination is essential to establishing a forward looking and consistent approach that provides clear guidance to providers whose networks form the technical foundation of 5G. Telecommunications providers, whose fiber will lay the foundation for 5G devices, often must budget and plan for deployment a year in advance, especially in rural areas where the weather and terrain restrict laying fiber to a few months out of the year. Smaller providers also operate with tight budgets that do not allow for replacing equipment outside of the normal life cycle if equipment should be deemed a threat to national security, and thus be required to be removed, after being released commercially. Consequently, a coordinated approach among the federal agencies tasked with protecting national security in order to prospectively identify equipment that poses a threat is essential to advancing 5G deployment. A coordinated approach will simultaneously streamline federal agencies' burden in developing policies that account for the complicated and extremely important nature of protecting the individuals, products and facilities that use 5G.

- **Dell Technologies Inc. [p. 6]:** Domestically, the relevant agencies should coordinate with private entities to help mitigate supply chain risk. One example of existing coordination efforts in this area includes the Information and Communications Technology Supply Chain Risk Management Task Force, managed by the Department of Homeland Security. This and future public-private partnerships will effectively develop recommendations to identify and manage risk in the global supply chain. Future task forces should provide for secure information sharing systems to manage cyber and other related threats to 5G infrastructure. Ultimately, a well-coordinated inter-agency partnership with private entities is critical to providing and maintaining an effective supply chain risk management plan.
- **Global Technical Systems [p. 3]:** Without direct Government support, US industry cannot achieve manufacturing capacities necessary to compete globally. As the US operates in conjunction with our allies around the world, the security of their ICT architectures is also a significant vulnerability. As a result, our second level recommendation suggests the need for Commerce to work hand-in-hand through an established taskforce with the DoD and industry. Shared responsibility and resourcing are recommended to establish funding to increase industrial capacity in identified critical microelectronics technology arenas.
- **Gigamon [p. 2]:** Gigamon believes that incentives will encourage earlier and more robust participation from organizations other than service providers and 5G equipment manufacturers who may have specific industry needs which should be addressed by emerging 5G standards. For example, the banking industry currently uses 3GPP network connections for a majority of consumer transactions, which makes authenticating customers using mobile identity challenging for both themselves and the service providers. In addition, automobile manufacturers are increasingly developing equipment that is highly dependent on mobile connectivity. Ensuring adequate information assurance over these channels will be critical as lives will be at stake. These are just two examples of industries that should engage but there are many more.

Theme: Security Principles

Summary: Several commenters provided examples of security principles developed by their associations for consideration. Ensuring transparency and open communication between different stakeholders is needed to identify problems as they arise. End-to-end trust of all elements of a network is needed to mitigate concerns of weak points in hardware or software. A certification process can be used to test security and reliability of all components from 5G suppliers.

RFC Response Examples:

- **GSM Association [p. 6]:** Any security scheme should ensure that operators are able to continue to identify and share problems as they arise and work together for secure, reliable networks across borders. Efforts such as the Criteria for Security and Trust in Telecommunications Networks and Services from the Center for Strategic & International Studies (CSIS) show great promise and complement both the Prague Proposals and the European Union's 5G Toolbox.
- **JMA Wireless [p. 6]:** JMA believes that ensuring end to end communication, both within internal 5G networks as well as adjacent allied networks overseas should remain a top priority. All elements of these networks must be trusted end-to-end. A single point of weakness, provided by untrusted hardware or software development origin is a cause for concern and should be safeguarded. Requiring some level of domestic manufacturing and software coding in the most critical elements, those managing user data or transmission,

supports a security framework that can be tracked, audited and mitigated more quickly than a highly distributed global supply chain of solutions.

- **Tenet3 [p. 1]:** Tenet3 recommends the adoption of risk assessment and security principles inspired from publications of the Department of Defense's previous work under the Anti-Tamper and Software Protection Initiative (ATSPI). The principles are rooted in an Electronic Warfare Threat Model where system vulnerabilities are assessed based on the enumeration of (i) critical system components and their susceptibilities; (ii) access points, resulting attack paths, and accessible data and functions needed to expose these susceptibilities, and (iii) technical capabilities enabled by the operating environment to leverage (i) and (ii) for an exploit.
- **Toshiba [p. 3]:** The Joint Commenters believe that 5G ecosystem participants must adopt a posture of quantum readiness and defense-in-depth countermeasures to address the challenges quantum computers will pose. We urge NTIA to refrain from mandating the specific type(s) of post-quantum protection for 5G networks. Instead, the Joint Commenters support steps by NTIA to encourage a focus on crypto-agility that will enable 5G network providers to deploy quantum-safe alternatives in advance of the emergence of quantum computing and to adjust to threat as they develop.

Line of Effort 3: Address Risks to United States Economic and National Security During Development and Deployment of 5G Infrastructure Worldwide

Theme: Vendor Diversity

Summary: Many commenters noted the importance of fostering vendor diversity across the 5G network and applications ecosystem and supply chain, and the benefits of such diversity that extend beyond securing domestic 5G infrastructure. There were some concrete suggestions of how to promote such diversity offered by respondents.

RFC Response Examples:

- **JMA [p. 9]:** JMA recommends the Federal Government look at multiple constructs to support vendor diversity and foster market competition. Incentives to small development companies should be considered as well as leveraged both by the Federal Government in their own 5G internal networks, state and local governments, and critical infrastructure.
- **CTIA [p. 2]:** Adopt a more strategic and forward-looking approach to include investing in 5G infrastructure, supporting private sector research and development ("R&D"), and pursuing creative and collaborative financing with like-minded allies to promote vendor diversity and respond to other countries' industrial policy.
- **Information Technology & Innovation Foundation [p. 2]:** It is critical networks are built with secure components. A ban on Chinese 5G equipment makes sense; a ban on exports to Huawei does not. A better strategy should drive wireless innovation beyond 5G, with equipment from a diversity of suppliers.
- **City of New York [p. 4]:** The City also encourages the federal government to promote 5G vendor diversity and foster market competition, so long as these actions do not negatively impact or otherwise disrupt paramount security considerations and initiatives.

- **JEITA [p. 2]:** Technologies will continue to evolve and advance during the 5G rollout period. To ensure that the 5G infrastructure allows the various 5G carriers and private 5G systems to connect with each other seamlessly and readily substitute their products, it is essential to avoid vendor lock-in by adopting common architecture agreed among the stakeholders both in public and private sectors.

Theme: U.S. Sourcing of Critical Components

Summary: Commenters called for identification of critical components by the U.S. government and for it to take steps to ensure that these components are sourced in the United States.

RFC Response Examples:

- **Mavenir [p. 5]:** The U.S. must continue to encourage manufacturing of semi-conductors in the U.S. and should provide incentives for companies to locate manufacturing within the U.S.
- **Aviat Networks [p. 1]:** These steps [to enable environment that supports U.S. innovation] should include prioritizing U.S. based manufacturing by U.S. companies, using targeted government/public funding to complement private sector U.S. investment to accelerate the rollout of 5G infrastructure, investing in U.S. workforce training and development of new U.S. based technology.
- **U.S. Ignite [p. 2]:** The dramatic increase and escalation of cyberattacks against a variety of organizations demonstrates that in developing a 5G architecture, security should not be considered after the fact. US Ignite recommends the federal government, in particular the Department of Defense (DOD) and the Department of Homeland Security (DHS), should co-lead establishing the necessary security standards & requirements for domestic and overseas operations to ensure National Security. The requirements will need to drive the necessary supply chains to ensure the domestic supply of RF components, integrated chips sets, devices and services are secure.
- **Global Technical Systems [p. 3]:** Based on the threat assessment, provide prioritized identification of hardware, firmware and software that represents the greatest potential for exploitation and designate such capabilities for US-only supply sourcing for US 5G network components.

Theme: Supply Chain Transparency

Summary: Respondents suggested that ensuring supply chain transparency is an important goal necessary to achieving the Strategy. While some noted the difficulties of such transparency, others made concrete suggestions as to how to achieve this goal.

RFC Response Examples:

- **Blackberry [p. 5]:** Also inherent within the framework is the need for a robust supply chain risk management system (SCRM). To truly trace and track an entire supply chain for a product a manufacturer must be able to maintain a serialized track and trace (STT) process.
- **Nokia [p.13]:** If, however, policymakers do not have fundamental trust that the supplier is compliance oriented or if there are concerns that the supplier lacks transparency of ownership and management decision-making or may be influenced by third party actors then, regardless

of the quality of the products and the security processes, mitigation of risk becomes more difficult.

- **Information Technology Industry Council [p. 5]:** Any policy intended to address challenges related to 5G security should be risk-based, evidence-based, adaptable, and fit-for-purpose. To the extent that governments continue to focus on supply chain security in the context of 5G deployment, they should either undertake or promote risk assessments to gain fuller visibility into the threat landscape, including the supply chain ecosystem and which risks can be mitigated and which ones cannot.

Theme: Interoperability

Summary: Many commenters highlighted interoperability as a key to promoting vendor diversity and security of the American 5G networks. Most called for a coordinated approach between industry and the government. Several comments noted that beyond financial incentives, the federal government could set an example by procuring equipment that adheres to international interoperability standards for its own networks. Some accentuated the federal government's role in leading the push toward interoperability among the global community.

RFC Response Examples:

- **Semiconductor Industry of America [p. 6]:** In order to promote vendor diversity, the government should focus efforts on promoting the greater use of open and interoperable interfaces, without mandating their use. First, as the government procures radio access network equipment, it should keep the procurement process open to equipment that uses open interfaces. Additionally, the government should signal that it supports the use of interoperable RAN systems. For example, the FCC is currently engaged in a proceeding to develop a framework to replace equipment in operators' networks. As the FCC develops its framework for communications equipment, they should include open RAN based solutions on the list, as well as established solutions from allied vendors.
- **Internet & Television Association [p. 10]:** Technical research and development, product testing, and global standards and specifications around security and interoperability are crucial to bolstering 5G security implementation and innovation.
- **Partnership for Interoperable Networks [pp. 4, 5]:** For government-owned networks, procure network equipment that adheres to international standards for interoperability, where appropriate…. Encourage the private sector to engage in the continued development of international standards for network interoperability. Liaise with international partners to ensure a coordinated approach to adoption.

Theme: Open RAN (ORAN)

Summary: Among the calls for interoperability, ORAN is the most notable in comments. Commenters argued that ORAN promises to deliver new opportunities for U.S. companies of all sizes to compete in the 5G market, thus stimulating vendor diversification. Some respondents called for a reduction of reliance on foreign-based providers of proprietary technologies. Also highlighted was specific ORAN-friendly legislation, such as the USA Telecom Act, as possible means through which to foster ORAN development.

RFC Response Examples:

- **NEC Corporation [p. 3]:** Pursing Open RAN approaches will present new opportunities for U.S companies from enterprises to start- ups to enter the market and compete. This represents a proven ability to introduce further vendor diversification in the United States providing alternatives to the existing traditional vendors.
- **Telecom Infra Project [p. 5]:** Legislation like the USA Telecom Act, that fosters innovation and competition within the 5G technology ecosystem by supporting Open RAN R&D and open-architecture wireless technologies, is key to driving vendor diversity and greater competition.
- **Open RAN Policy Coalition [p. 4]:** In short, open RAN provides the framework for these communications network stakeholders to align on shared understanding of security requirements and to tailor security requirements at a more granular level than has been possible before. Additionally, 5G and an open RAN also enable new capabilities and control points that allow suppliers, test equipment manufacturers, wireless carriers, and network operators to assess and to manage security risks. Because an open RAN is a fundamentally open architecture, it opens the ecosystem to new suppliers, increasing the diversity of virtualized RAN solutions.
- **Blue Danube [p. 11]:** Key industry stakeholders are pushing once again to establish an open interface to the radio. The Open Radio Access Network (ORAN) Committee has excellent support in the industry and is working to develop a more robust open interface to the radio. Most significant OEMs participate in this effort, as well as many smaller companies, including Blue Danube.
- **Cisco [p. 7]:** To be clear, we are not calling for government mandates; we do not want the U.S. government—or any government—to force a shift to open RAN or any other approach to building a network. Instead, we urge the U.S. government to promote a regulatory model that provides for streamlined deployment and encourages diversity and choice among rigorous standards-based innovations in the market of trusted suppliers.

Theme: Accreditation and Certification

Summary: Some commenters recommended new, or better utilizing existing, accreditation and certification schemes run by either the U.S. government or the private sector to secure 5G infrastructure and supply chain.

RFC Response Examples:

- **American National Standards Institute [p. 8]:** ANAB encourages the use of existing private sector certification programs to address the security of the telecommunications infrastructure supply chain. For example, the FCC Telecommunications Certification Body (TCB) program is an equipment authorization procedure that provides for effective and efficient testing and certification of Radio Frequency (RF) devices prior to being marketed or imported into the United States.
- **Keysight Technologies [p. 7]:** Requiring independent source code and component validation. Additionally, the use of open-source code should be encouraged wherever possible because even an otherwise secure piece of hardware or software may be rendered insecure by the inclusion of a single component or software library… Mandating a certification process to a set of testing standards for security and reliability that is required by

all suppliers of 5G hardware and software. A certification process is a very useful tool to improve security of the supply chain and 5G ecosystem similar to the UL certification conformance model.

- **FEDDATA [p. 5]:** One industry proven approach for incentivizing improvements is by certification of adherence to a mandatory Maturity Model. This approach would promote a level competitive playing field, evolve, and adapt to changing threats and enforce requirements that are critical to eventual desired security outcomes.

Line of Effort 4: Promote Responsible Global Development and Deployment of 5G

Theme: Standards

Summary: Commenters highlighted the history of American leadership in the development of 4G standards as a reason for U.S. preeminence in global telecommunications, pointing then to the urgency of maintaining representation in international standards-setting bodies. Respondents highlighted funding as a means to encourage the private sector's participation in the standards arena. Some suggested making the United States a more attractive venue for standards setting bodies as a means to decrease the cost of participation for U.S. companies. Some commenters also called for the U.S. government to act as a convener to help ensure that the private sector is able to prioritize and coordinate standards participation. The 3GPP and International Telecommunications Union were both noted as priority organizations for U.S. involvement.

RFC Response Examples:

- **ANSI [pp. 4, 7]:** The international wireless communication systems standards space is multifaceted – it encompasses a range of organizations such as the 3rd Generation Partnership Project (3GPP), the global collaborative effort comprising seven standards development organizations (SDOs) that draw up complete mobile system specifications, including the Long-Term Evolution (LTE), LTE-Advanced and 5G wireless specifications; the Internet Engineering Task Force (IETF); and the International Telecommunication Union (ITU). Also important are the World Wide Web Consortium (W3C), Institute for Electrical and Electronics Engineers (IEEE) and the O-RAN Alliance, just to name a few key players… ANSI National Accreditation Board recommends that international conformity assessment standards, ISO/IEC 17011, ISO/IEC 17024, ISO/IEC 17025, and ISO/IEC 17065 be referenced to recognize accreditation bodies, testing laboratories, and certification bodies in the National Strategy to Secure 5G Implementation Plan.
- **NEC Corporation [p. 5]**: To effectively promote a diverse, competitive supply chain of trusted, secure, open and interoperable technologies, the implementation could consider leveraging U.S. State Department and U.S. international funding agencies, along with partnerships with similar organizations like the Japan Bank for International Cooperation (JBIC) and Nippon Export and Investment Insurance (NEXI) to include preferences for open, interoperable and standards based equipment in wireless projects that will result in the deployment of open interoperable network equipment from trusted vendors and service providers.
- **Telecommunications Industry Association [p 13]:** The U.S. government should work towards making the U.S. the best, most welcoming place to develop standards and coordinate

international standards development projects. This has direct benefits to the ability of American companies to participate in and lead standards by:

- decreasing travel, lodging, and incidental costs associated with attending internationals standards development meetings abroad;
- lowering perceived barriers to entry for U.S. small and medium enterprises; and
- giving American participants a "home-field advantage" where they can operate in their native time zone and language.

- **Nokia [p. 11]:** Nokia recommends that the U.S. seek ways to reduce the costs of acquiring participation rights in key standards bodies as well as easing costs of sending experts to participate in working groups and of developing intellectual property to support the standards. Specifically, we recommend that the Administration direct the Internal Revenue Service to issue clarification that costs of participation in standardization are recognized for favorable treatment under the R&D tax credit and providing guidelines for the types of expenses that can be recognized. Nokia also suggests that NIST explore ways to reduce the costs of obtaining voting memberships in key standards bodies through collaboration with the entities that provide such rights. It may also be appropriate to provide modest funding for grants to acquire voting memberships in standards bodies.
- **Alliance for Telecommunications Industry Solutions [pp. 7, 11]:** It is ATIS' view that the development of standards that support U.S. needs must be closely coupled with a broader strategy that connects research, development, manufacturing and commercialization objectives. Greater collaboration between U.S. Government, industry and standards coordination groups, such as ATIS, is also essential. To promote U.S. leadership on 5G and beyond, ATIS believes that the vital role played by global standards development must be recognized and encouraged. To this end, ATIS urges the U.S. Government to clarify that R&D tax credits apply to the development of next generation standards and the assessment of future technologies and architectures… Government can also play an important convening role in pulling industry together to determine if there is a need for incentives to continue to participate in standards bodies, to ramp up U.S. private sector representation and determine what those incentives may be (research and development tax credits, direct funding support, etc.).
- **Commonwealth Cyber Initiative [p. 5]:** Organizing a recurring national dialog between academia, private sector, government, around the country's priorities in 5G and beyond, and promoting and funding the representation of national priorities in the 3GPP standards process. Universities can play a key role as conveners.
- **Competitive Carriers Association [p. 5]:** Importantly, international standards can introduce both helpful technologies and potential risks to our networks. Thus, it is imperative that the U.S. is adequately represented on all standards setting bodies. The U.S. must have leadership representation within such bodies, as well as a close public/private partnership with the industry, to ensure appropriate standards that address potential risks are developed.
- **SecureG [p. 9]:** U.S. companies don't take a long-game approach to supporting its representatives in standards committees and treat their experts as the most dispensable when the company runs into hard times. Where the U.S. Government can help is by taking a strategic approach to the communications sector as a key element of its economic security. This means funding companies to find its best experts and taking a long-term commitment to

their participation. Contract vehicles such as Small Business Innovation Programs can be part of the answer even extending this form of contract to the larger businesses to hire and keep the standards experts.

Theme: The Prague Proposals

Summary: Many respondents noted that a primary vehicle for advancing international cooperation on secure 5G would be to promote international adoption and implementation of the Prague Proposals.

RFC Response Examples:

- **U.S. Chamber of Commerce [p. 7]:** The Chamber supports the Prague Proposals endorsed at last year's Prague 5G Security Conference. These recommendations were developed by cybersecurity officials from multiple countries, linked by common interests and collective activities, to counter threats and provided recommendations for nations to consider as they design, construct, and administer their 5G infrastructure. The Prague Proposals emphasize the need for 5G networks to be constructed based on free and fair competition, transparency, and rule of law, and they were recently personified in the U.S.-Poland Joint Declaration on 5G. We welcome the international collaboration embodied in the process that led to the initial Prague Proposals and look forward to future engagement.
- **Samsung Electronics America [p. 5]:** Samsung recommends that the U.S. Government collaborate with governments around the world to raise awareness of the importance of deployment of trusted and secure global 5G infrastructure. This includes encouraging the international community toward operationalizing the 5G security recommendations from the May 2019 Prague 5G Security Conference (the "Prague Proposals"). By using the Prague Proposals as a foundation for policymaking, global governments can further promote procurement of trusted and secure 5G equipment.
- **USTelecom [p. 6]:** In particular, the National Strategy to Secure 5G should reflect and affirm the principles and goals of the "Prague Proposals for 5G," a set of recommendations aiming to promote a diversity of market participants in lieu of only few dominant players that can pose threats to national security. The Prague Proposals, which were developed by the United States and thirty-one other countries, are premised on the rule of law, independent judiciary, corporate transparency and accountability, and security by design.

Theme: Export-Import Bank

Summary: A few of the commenters pointed out the need for a more flexible approach to the U.S. funding of the secure and trusted global 5G infrastructure, particularly through leveraging the Export-Import Bank of the United States. This strategy was highlighted as a viable way for the U.S. to combat Chinese government subsidies.

RFC Response Examples:

- **Semiconductor Industry of America [p. 8]:** EXIM should adopt a more flexible approach to U.S. content rules that might include taking into account U.S. R&D and IP, as well as significantly lowering U.S. content requirements to support the national security priority to finance deployment of secure and trusted telecommunications infrastructure.

- **U.S. Chamber of Commerce [p. 9]**: Fostering secure and trusted 5G infrastructure can be strengthened by leveraging the Export-Import Bank of the United States' (EXIM) financial products to directly neutralize export subsidies offered by the People's Republic of China.
- **Computing Technology Industry Association (CompTIA) [p. 3]:** Building on the State Department's work on global 5G supply chain security issues via the Prague Proposals, the federal government should establish a Multilateral Telecom Security Fund, as envisioned in recent legislation introduced in Congress. It should also revise the U.S. International Development Finance Corporation rules to support strategic investments in 5G technologies in Europe and Eurasia, revise the U.S. Export-Import ("EXIM") Bank rules to support trusted suppliers, and expand the federal R&D tax credit to encompass participation in standards development activities while avoiding politicization of the standards process.

Theme: Intellectual Property

Summary: Many of the industry and industry association comments called for increased attention to intellectual property policies, noting, in particular, the need for the U.S. to take the leading role in this area. Most encouraged the government to take a more active role in fostering innovation among the U.S. enterprises and taking an aggressive stance protecting American intellectual property in the global markets. Several comments also noted the role of sound IP policies in setting the stage for the development of 6G networks.

RFC Response Examples:

- **Ericsson [p. 25]:** Other countries look to the U.S. for guidance on issues relating to global standards and FRAND licensing. We encourage the continued support for policies that reflect these important principles and provide a clear, balanced and unified message on the importance of respect for IP protections, U.S. private sector leadership in open, transparent, and voluntary consensus-based SDOs, and robust support for FRAND licensing commitments.
- **Information Technology and Information Foundation [p. 2]**: Policymakers should increase funding for early stage wireless R&D, setting the stage for 6G; support fair processes in standards-setting organizations; assist allies to see a larger market for trusted vendors; and protect IP rights for innovators.
- **Raytheon [p. 8]:** As networks operate both domestically and internationally, there is always a risk companies will lose intellectual property ("IP") due to bad actors. Protection of IP is a key driver for vendors operating internationally. The U.S. Government should (1) advocate for aggressive protection of U.S. technology IP rights and (2) promote domestic innovation by fostering private enterprise IP.