Coalition for Cybersecurity
Policy & Law

Coalition for Cybersecurity Policy & Law
600 Massachusetts Ave, NW, Washington, DC 20001

February 12, 2018

VIA EMAIL: counter_botnet@list.commerce.gov

Evelyn L. Remaley
Deputy Associate Administration
National Telecommunications and Information Administration
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

Re: Comment of the Coalition for Cybersecurity Policy & Law on the *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*

The Coalition for Cybersecurity Policy & Law ("Coalition") submits this comment in response to the Request for Comments ("RFC") issued by the Department of Commerce ("DoC"), regarding the *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* ("Report"). The Coalition appreciates the opportunity to provide feedback on the Report.

The Coalition is comprised of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[1] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management, and we are supportive of efforts to identify and promote the adoption of cybersecurity best practices and voluntary standards throughout the global community.

Representatives of Coalition member companies actively participated in the workshop hosted by the National Institute of Standards and Technology ("NIST") that was held to inform this report.

The Coalition broadly supports and agrees with the findings and recommendations of the report. In particular, we commend the Department of Commerce and the Department of Homeland Security ("DHS") for repeatedly and effectively highlighting the importance of public and private collaboration, as well the international policy and standards development and adoption that are essential to long term success.

[1] The views expressed in this comment reflect the consensus view of the Coalition and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, *see* www.cybersecuritycoalition.org.

In support of this, the Coalition intends to host an event bringing together government and private sector leaders and experts to further discuss this important issue and drive progress.

In regards to Action 2.2, the Coalition notes that it has previously provided NIST with a DDoS Mitigation and Prevention Profile based on the combined experience and expertise of its member companies, who include providers that offer a range of services specifically designed to achieve the stated goal. We look forward to working with NIST and other private and public sector partners to expand and refine this Profile.

Additionally, we believe that a Botnet Prevention and Mitigation Profile is a necessary addition to the body of available knowledge, and would be highly complementary to the DDoS Mitigation and Prevention Profile discussed. To that end, the Coalition is providing a Profile for your consideration and to help foster conversation within the broader community.

Conclusion. The Coalition thanks the Department of Commerce and the Department of Homeland Security for its leadership in coordinating this important effort and for the opportunity to comment.

Cybersecurity Framework DDoS and Botnet Prevention and Mitigation Profile(s)

Executive Summary

The Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) version 1.0, developed by the National Institute of Standards and Technology (NIST), with extensive private sector input, provides a risk-based and flexible approach to managing cybersecurity risk that incorporates industry standards and best practices. The Cybersecurity Framework is by design crafted to allow individual organizations to determine their own unique risks, tolerances, threats and vulnerabilities, so that they may prioritize their resources to maximize effectiveness.

The Framework is general in nature to allow for broad applicability to a variety of industries, organizations, risk tolerances and regulatory environments. A Framework Profile is the application of Framework components to a specific situation. A Profile may be customized to suit specific implementation scenarios by applying the Framework Category and Sub-Categories appropriate to the situation. Profiles should be constructed to take into account the organization's:

- Business/mission objectives
- Regulatory requirements
- Operating environment

Organizations can use Profiles to define a desired state for their Cybersecurity posture based on their business objectives, and use it to measure progress towards achieving this state. It provides organizations with the ability to analyze cost, effort and risk for a particular objective. Profiles may also be used by industry sectors to document best practices for protection against specific threats.

The below Cybersecurity Framework Profile focuses on Distributed Denial of Service (DDoS) and botnet prevention and mitigation. DDoS attacks are increasing in complexity, size, and frequency. Botnets have long been used as a method for orchestrating DDoS and other attacks. The range of targets and methods (e.g., from using individual PCs to using connected Internet of Things (IoT) devices) has also broadened. These threat profiles emphasize how the Cybersecurity Framework can address DDoS attacks and prevent and mitigate devices that have become parts of a botnet.

To develop the threat profile, we have reviewed all the Cybersecurity Framework Categories and Subcategories and determined those most important to combat the DDoS and botnet threats. The Categories and Sub-Categories were then labeled into different priorities as follows:

P1 – Minimum actions required to protect network and services against relevant attacks.

P2 – Highly recommended actions to protect network and services against relevant attacks.

P3 – Recommended actions to protect network and services against relevant attacks.

The DDoS and Botnet threat mitigation profile represents a Target Profile focused on the desired state of organizational cybersecurity to mitigate DDoS and botnet threats. It may be used to assist in identifying opportunities for improving DDoS and botnet threat mitigation and aiding in cybersecurity prioritization by comparing current state with this desired target state.

The Coalition developed this profile based on version 1.0 of the Cybersecurity Framework. The comments provided as part of the profile give appropriate guidance to refine the understanding of relevant Framework subcategories as they apply to DDoS and botnet threat mitigation. While Coalition members believe that Framework version 1.0, and its associated Core categories and subcategories, allow for adequate flexibility to develop an effective DDoS threat mitigation profile, we welcome the updates in draft 2 of version 1.1 of the Framework, as they reflect changes in the evolving nature of cybersecurity threats and risk management practices, which can further assist organizations in defending against and mitigating DDoS attacks.

Examples of beneficial changes in draft 2 include updates in Section 3.0 ‘How to Use the Framework’ on how the Framework can be applied in design, build/buy, deploy, operate, and decommission system lifecycle phases. Cybersecurity practices must be considered throughout the full range of information technology activities of organizations as industries across all sectors increasingly develop and leverage IT applications and connected devices. In addition, new Framework Core categories and subcategories focused on managing supply chain risk will help organizations better defend against key threat vectors for DDoS attacks.

Overview of the DDoS and Botnet Threats

A DDoS attack attempts to overwhelm a network, service or application with traffic from multiple sources. There are many methods for carrying out DDoS attacks. These can include

- Low bandwidth connection-oriented attacks designed to initiate and keep many connections open on the victim exhausting its available resources.
- High bandwidth volumetric attacks that exhaust available network or resource bandwidth.
- Protocol oriented attacks that take advantages of stateful network protocols such as TCP.
- Application layer attacks designed to overwhelm some aspect of an application or service.

Although each of these methods can be highly effective, in recent years, there has been considerable attention given to volumetric attacks as the result of several high-profile incidents.

One prominent example of a volumetric DDoS attack vector is reflection amplification. This is a type of DDoS attack in which the attacker fakes the attack target’s IP address and launches queries from this address to open services on the Internet to solicit a response. The services used in this methodology are typically selected such that the size of the response to the initial query is many times (x100s) larger than the query itself. The response is returned to the real owner of the faked IP. This attack vector allows attackers to generate huge volumes of attack traffic, while making it difficult for the target to determine the original sources of the attack traffic. Reflection amplification has been responsible for some of the largest DDoS attacks seen on the Internet through the last decade.

DDoS is often referred to as a ‘weaponized’ threat as technical skills are no longer needed to launch an attack and services to conduct DDoS have proliferated and become easily obtainable for relatively low cost. Attackers can build out their attack capability in many ways, such as the use of malware to infect Internet connected computers, deploying servers within hosting environments, exploiting program flaws or other vulnerabilities, and by exploiting the use of inadequate access controls on Internet connected devices to create botnets.

Botnets are created when an attacker infects or acquires a network of hosts, then controls these devices to remotely launch an attack at a given target. Increasingly, botnets are incorporating Internet of Things (IoT) devices, which continue to proliferate at a remarkable rate. Botnets allow for a wide variety of attack methods aimed at evading or overwhelming defenses. Compromised devices within an organization can be used by the botnet to carry out attacks; DDoS or otherwise, targeting assets and infrastructure inside or outside the organization. This can have a significant negative impact on the overall risk posture of the organization and its reputation and responsibility in the community. The United States continues to be the most frequent target of DDoS attacks and infected hosts within the US public and private infrastructure are most frequently leveraged as the source of DDoS and botnet attacks. Availability is a core information security pillar but the operational responsibility and discipline for assessing and mitigating availability-based threats such as DDoS often falls to network operations or application owners in addition to Risk and Information Security teams. Because of this divided responsibility, fissures in both risk assessment and operational procedures for addressing these threats may occur. The goal of this profile is to ensure the strategic and operational discipline needed to protect and respond to DDoS threats is comprehensively addressed by applying the appropriate recommendations and best practices outlined in the Cybersecurity Framework.

APPENDIX A

DDoS Threat Mitigation Profile

Function	Category	Sub-Category	Priority	Framework Comment
Identify (ID)	Asset Management (ID.AM)	**ID.AM-1:** Inventory physical devices and systems within the organization	**P2**	Catalog critical Internet facing services by location and capacity Catalog ISP connectivity by ISP, bandwidth usage, bandwidth available
		ID.AM-2: Inventory software platforms and applications within the organization	**P1**	Determine critical Internet facing services by type of application/service, IP address and hostname, and determine which open source software components are used across applications.

Function	Category	Sub-Category	Priority	Framework Comment
		ID.AM-3: Map organizational communication and data flows	**P2**	Identify key stakeholders in the organization critical to availability of Internet facing services including application owners, security personnel, network operations personnel, executive leadership, legal/risk personnel and ISP or Cloud based DDoS mitigation service providers Maintain network maps showing data flows Create an operational process document detailing communication workflows
		ID.AM-4: Catalogue external information systems	**P3**	Identify applications and services that are run in cloud, SaaS, hosting or other external environments
		ID.AM-5: Resources are prioritized based on their classification, criticality, and business value	**P2**	Determine what Internet facing services will result in the most business impact if they were to become unavailable
	Business Environment (IDE.BE)	**ID.BE-4:** Establish dependencies and critical functions for delivery of critical services	**P2**	Catalog external dependencies for services and applications including DNS, NTP, cloud/hosting provider, partner network connections and Internet availability
		ID.BE-5: Establish resilience requirements to support delivery of critical services	**P3**	Ensure geographical redundancy and high availability of equipment providing services, network infrastructure and Internet connections

Function	Category	Sub-Category	Priority	Framework Comment
	Risk Assessment (ID.RA)	**ID.RA-1:** Identify and document asset vulnerabilities	P2	Determine network and application bottlenecks including throughput, connection rate and total connections supported
		ID.RA-2: Cyber threat intelligence and vulnerability information is received from information sharing forums and sources	P3	Monitor vulnerabilities lists (CVE, NVD and similar) to check if critical Internet facing services have vulnerabilities that could be used as a condition for Denial of Service.
		ID.RA-3: Identify and document internal and external threats	P3	Continuously gather industry information around DDoS trends, peak attack sizes, frequency, targeted verticals, motivations and attack characteristics
		ID.RA-4: Identify potential business impacts and likelihoods	P2	Create a risk profile that quantifies potential cost of recovery operations per DDoS incident, revenue loss, customer churn, brand damage and impact to business operations
	Governance (ID.GV)	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	P1	Put processes in place to ensure all regulatory requirements are met. Train all personnel responsible for DDoS incident response on the relevant legal and regulatory requirements surrounding the data that they may handle. Document regulatory and data privacy policies of DDoS service providers and partners

Function	*Category*	*Sub-Category*	*Priority*	*Framework Comment*
Protect (PR)	**Awareness and Training (PR.AT)**	**PR.AT-2:** Privileged users understand roles & responsibilities	P1	Security Operations personnel have been trained on DDoS defense processes, products and services Equip security operations personnel with an operational run book defining what process to follow and who to contact should an incident take place
	Information Protection Processes and Procedures (PR.IP)	**PR.IP-1:** Create and maintain a baseline configuration of information technology/industrial control systems	P1	Create a baseline DDoS protection architecture consisting of best current practices for the network, network based protection capabilities and non-stateful Intelligent DDoS Mitigation capability Implement anti-spoofing and black/white list filtering at network edge Maintain DDoS protection configuration that provides general protection for all services and always on protection for all business-critical assets
		PR.IP-7: Continuously improve protection processes	P2	Conduct a minimum of 2 annual tests of DDoS protection capabilities Perform after-action reviews following all DDoS incidents and DDoS protection tests adjusting DDoS defenses accordingly

Function	Category	Sub-Category	Priority	Framework Comment
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	P3	The organization's Business Continuity and Disaster Recovery plans should have components to address the potential effects of a DDoS attack
		PR.IP-10: Response and recovery plans are tested	P3	The DDoS components of the Business Continuity and Disaster Recovery plans should be tested.
		PR.IP-12: A vulnerability management plan is developed and implemented	P3	Vulnerabilities that can be leveraged for DDoS events should be documented and remediated.
	Protective Technologies (PR.PT)	**PR.PT-4:** Protect communications and control networks	P1	Perform filtering of traffic to control plane network and/or control plane traffic policing
Detect (DE)	**Anomalies and Events (DE.AE)**	**DE.AE-1:** Establish and manage a baseline of network operations and expected data flows for users and systems	P1	Continuously measure traffic to hosts, resources or groups of resources to determine expected traffic over time. Determine traffic baselines at IP layers 3 and 4 including IP bandwidth, TCP, UDP, ICMP, GRE, and at the application level including critical applications such as HTTP, HTTPS, DNS, NTP, SSDP and SIP
		DE.AE-2: Analyze detected events to understand attack targets and methods	P1	Determine source and destination traffic characteristics when anomalous traffic is

Function	*Category*	*Sub-Category*	*Priority*	*Framework Comment*
				detected that is indicative of DDoS
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	P2	Aggregate data for detected DDoS events from multiple network sources contributing to the attack.
		DE.AE-4: Impact of events is determined	P2	Total traffic rates for DDoS events can be measured across all contributing network sources Performance and availability of services can be measured before, during and after events
		DE.AE-5: Incident alert thresholds are established	P1	Configure notifications to security monitoring personnel and appropriate stakeholders when traffic exceeds measured or configured thresholds
	Security Continuous Monitoring (DE.CM)	**DE.CM-1:** Monitor network to detect potential cybersecurity events	P1	Continuously measure traffic install network ingress points and between transit points on the internal network for traffic anomalies To the extent possible and/or practical from a business perspective, continually measure outbound traffic for detection of traffic anomalies that could represent sources contributing to outbound or cross-bound DDoS attacks.

Function	Category	Sub-Category	Priority	Framework Comment
		DE.CM-8: Vulnerability scans are performed	P1	Scan Internet facing services and software applications to identify vulnerabilities that can be exploited for participation in DDoS events.
	Detection Processes (DE.DP)	**DE.DP-3:** Test detection processes	P2	Conduct regular testing of DDoS defense capabilities including occasional unannounced tests performed with no prior warning to assess the DDoS defense strategies and processes Conduct DDoS simulation wargames as part of security staff onboarding and periodically for the security response team
		DE.DP-5: Continuously improve detection processes	P2	Perform after-action review on any defense testing or DDoS events after all operations are successfully restored to identify and improve DDoS detection capabilities Identify and maintain key security metrics around detection, identification and escalation effectiveness.
Respond (RS)	**Response Planning (RS.RP)**	**RS.RP-1:** Execute response plan during or after an event	P1	Follow DDoS response run book during any detected DDoS events
	Communications (RS.CO)	**RS.CO-1:** Ensure personnel know their roles and order of operations when a response is needed	P1	Define personnel responsible for detection, mitigation, coordination and communication during DDoS incidents

Function	Category	Sub-Category	Priority	Framework Comment
🟥		**RS.CO-4:** Coordinate with stakeholders consistently with response plans	P1	Document operational run book that includes roles, responsibilities and escalation process for all parties responsible for DDoS incident response including internal personnel and external consultants or services
		RS.CO-5: Engage in voluntary information sharing with stakeholders to achieve broader cybersecurity situational awareness	P3	Share and receive DDoS attack trends with consultants, service companies and/or threat intel companies to keep abreast of attack scale, frequency, motivations and evolving attack vectors
	Analysis (RS.AN)	**RS.AN-1:** Investigate notifications from detection systems	P1	Add DDoS alert notifications to monitoring and response systems including security and network operations management systems.
		RS.AN-2: Understand the impact of the incident	P2	Compare DDoS traffic rates, connection rates and total connections against documented system and network limits Identify actual and potential impact to business services, customers, employees and other stakeholders.
		RS.AN-3: Forensics are performed	P3	Save raw anomaly details in available form (logs, packet captures, flow telemetry data) to investigate parties involved in the incident and, where appropriate, to share incident details

Function	*Category*	*Sub-Category*	*Priority*	*Framework Comment*
				with the operational security community.
	Mitigation (RS.MI)	**RS.MI-2:** Mitigate incidents	P1	Mitigate DDoS attacks using any or all of the following: - Network capabilities such as ACLs, anti-spoofing, remote triggered blackhole and/or flow spec - Using intelligent DDoS mitigation systems on premise - Contracting a DDoS mitigation service Critical resources should be protected by always on mitigation capabilities - Contract or coordinate with upstream bandwidth provider for defense against high-magnitude attacks. Implement a notification system to detect when on premise bandwidth is reaching saturation then alert and/or automate movement of traffic to an upstream DDoS mitigation service Identify and maintain key security metrics around mitigation and escalation effectiveness.

Function	*Category*	*Sub-Category*	*Priority*	*Framework Comment*
	Improvements (RS.IM)	**RS.IM-1:** Incorporate lessons learned into response plans	P2	Adjust mitigation processes, capacity, technology and partnerships based on DDoS attack trends, DDoS response testing and results of DDoS after-action reviews Maintain key security metrics around the DDoS program to demonstrate program improvement and effectiveness.
Recover (RC)	**Recovery Planning (RC.RP)**	**RC.RP-1:** Execute recovery plan during or after an event	P2	Establish an internal and external communication plan as part of the DDoS run book that is used every time there is a DDoS incident
	Communications (RC.CO)	**RC.CO-1:** Manage public relations	P2	Ensure impacted applications are restored and availability communicated to relevant stakeholders Manage external communications based on visibility and impact of the DDoS attack on customers, partners or public

Botnet Threat Mitigation Profile

Function	*Category*	*Subcategory*	*Priority*	*Comment*
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-1**: Physical devices and systems within the organization are inventoried	**P1**	Catalog all devices within the organization that have or have had direct or indirect access to the Internet.
		ID.AM-2: Software platforms and applications within the organization are inventoried	**P1**	Catalog all applications and services that have or have had direct or indirect access to the Internet.
		ID.AM-4: External information systems are catalogued	**P2**	Identify applications and services that are run in cloud, SaaS, hosting or other external environments.
	Risk Assessment (ID.RA)	**ID.RA-1:** Asset vulnerabilities are identified and documented	**P1**	All identified connected devices should be assessed for known vulnerabilities and that information should be documented and updated routinely.
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	**P1**	Monitor connected devices against known vulnerabilities (CVE, NVD and similar) and against a framework of regularly updated threat intelligence sources
		ID.RA-3: Threats, both internal and external, are identified and documented	**P3**	Continuously gather information regarding trends, attack characteristics, known vulnerabilities, and other Indicators of Compromise (IOC) through internal

				and/or external data sources.
PROTECT (PR)	**Access Control (PR.AC)**	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	**P1**	Controlling and managing access to connected devices is essential in preventing compromise and in mitigating compromised devices.
		PR.AC-3: Remote access is managed	**P2**	Authentication, authorization and accounting for any user access to the network and services must be established for local and remote access users. Multiple levels of access should be implemented to ensure users have access and control to only those things that they need to carry out their position. Network is segmented to allow only expected protocol and application traffic across different areas of the network.
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	**P2**	
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	**P3**	
	Data Security (PR.DS)			
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**P1**	Implement rigorous monitoring processes to detect devices that are no longer being used and remove these devices from

				the network to reduce potential attack surface.
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**P2**	Verify the authenticity and integrity of any updates that are applied to any devices on the network to reduce the likelihood of malicious code being uploaded to the device.
		PR.DS-7: The development and testing environment(s) are separate from the production environment	**P3**	Development environments can be less secure than production environments as they may host devices that are being tested or piloted and that have not yet been fully secured. Keeping the development and production environment separate can reduce risk.
	Information Protection Processes and Procedures (PR.IP)	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	**P1**	Creating a known baseline configuration for connected devices makes it easier to determine if unauthorized changes have been made.
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	**P2**	Implement a systems development lifecycle (SDLC) to build rigor into the purchasing, deployment, maintenance, and end-of-life processes for any devices connected on the network.
		PR.IP-3: Configuration change control processes are in place	**P1**	Configuration changes to connected devices should follow a rigorous process that requires authorization and tracking. Changes made outside this process may indicate a potential compromise.
		PR.IP-7: Protection processes are continuously improved	**P3**	Review protection processes on a routine basis to ensure that they are functioning as expected. Make adjustments when deficiencies are found.

		PR.IP-12: A vulnerability management plan is developed and implemented	**P1**	A comprehensive plan must be put in place for the identification and mitigation of software and hardware vulnerabilities. This will aid in quantifying risk and in identifying devices that require updates or replacement.
	Maintenance (PR.MA)	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	**P3**	Because maintenance requires access to connected devices, a process that requires approval and monitoring aids in the detection of unauthorized changes.
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**P3**	
	Protective Technology (PR.PT)	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**P1**	Routine review of audit logs is essential in being able to identify if unauthorized access or changes were made to devices on the network.
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	**P1**	Connected devices should be configured to allow only the access and privileges necessary to perform their intended function.
DETECT (DE)	**Anomalies and Events (DE.AE)**	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	**P1**	Maintain a baseline of network operations and data flows to enable detection of anomalous network behavior that could indicate a device has been compromised.
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	**P1**	Implement comprehensive monitoring across network infrastructure and individual network elements to detect events that are indicative of

		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	**P2**	a potentially compromised host. Implement an alerting mechanism to signal events to operations personnel. Implement an event aggregation system that will store all events and provide a level of triage and prioritization of events for operations personnel. Event monitoring should include the ability to detect the presence of malicious code on connected devices or in transit in the network and the presence of malicious traffic or device behaviors on the network.
	Security Continuous Monitoring (DE.CM)	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**P1**	
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**P2**	
		DE.CM-4: Malicious code is detected	**P1**	
		DE.CM-5: Unauthorized mobile code is detected	**P1**	
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**P3**	
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**P1**	
		DE.CM-8: Vulnerability scans are performed	**P1**	Conducting routine vulnerability scans of all connected devices and underlying software informs risk and provides direction on which devices and applications have the highest risk of compromise.
	Detection Processes (DE.DP)	**DE.DP-4:** Event detection information is communicated to appropriate parties	**P2**	Events related to connected devices that may be indicative of anomalous behavior should be communicated to

				appropriate parties for analysis and action.
		DE.DP-5: Detection processes are continuously improved	**P3**	Detection processes should be tested and reviewed routinely to ensure they are performing as expected.
RESPOND (RS)	**Communication (RS.CO)**	**RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**P2**	Multiple communities exist to share and analyze vulnerability and threat information for connected devices including industry consortiums, international CERT organizations, law enforcement, threat intelligence vendors, and operational security communities Participation within these entities can provide significant benefit in understanding how an organizations connected devices may be introducing risk and how best to mitigate it.
	Analysis (RS.AN)	**RS.AN-1:** Notifications from detection systems are investigated	**P1**	To the extent possible based on business and risk tolerance, alerts indicating potential infection of an infected host should be investigated by qualified personnel to determine risk. A system of triage and prioritization should be put in place to ensure that the most critical events are investigated first.
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**P1**	Vulnerabilities identified through scans, information sharing, or other analysis, should be documented immediately and either mitigated or treated as acceptable risk. When patching isn't viable,

🟥				mitigation may require complete removal and replacement of compromised device.