Purpose

This document intends to introduce the ISA BPS WG recommended approach to securing the BPS Supply Chain to the DOE in partial response to the Request for Information on "Securing Critical Electric Infrastructure"[1]. This document briefly discusses (two pages) the overall holistic approach to supply chain risk management (SCRM) and provides a one-page or shorter summary of each of the four program areas.

This paper is also being submitted to other federal and private sector stakeholders for widest consideration.

Introduction

Wouldn't it be nice if there was one simple, straightforward way to effectively manage Bulk Power System (BPS) supply chain risks? As many professionals in national security have had supply chain challenges in their sights for decades, chances are, if there were a silver bullet solution, we would have fired it by now. Overwhelming at first glance, a challenge of this magnitude and complexity can only be addressed by breaking it down into more-manageable pieces. In the words of former PJM CEO Terry Boston, silver buckshot is what is required for this type of problem not silver bullets.

Top-tier adversaries have become quite adept at orchestrating coordinated supply chain cyber attacks. Our defenses, particularly for the BPS, arguably the most critical of all critical national infrastructures, must be similarly coordinated. Federal and State government, suppliers, services providers, and asset owners all have important parts to play.

Until now, the lack of transparency in our supply chains has been perhaps the biggest impediment to progress. Suppliers sometimes cannot see a compromise within their production processes until it is installed in a customer's systems (SolarWinds). Asset Owners and Operators (AOOs) may have difficulty in tracing the pedigree of their installed ICS components, or quickly finding all instances of a particular ICS component when a vulnerability is discovered (RuggedCom, Emmerson, and many others).

At Issue – Lack of Transparency

Opaque SCRM processes have allowed adversaries to remotely access and manipulate our critical electric power infrastructure, evading detection. CIKR manipulation is contrary to national security interests and BPS reliability. The 2019 Worldwide Threat Assessment of the US IC confirmed as much:

"Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners.[2]"

[1] See https://www.energy.gov/oe/securing-critical-electric-infrastructure

[2] Worldwide Threat Assessment of the US Intelligence Community. January 29, 2019. On pg. 5. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Opportunity

The past several years has seen many Presidential Executive orders (EO) generated, several focused on adversarial manipulation of previously trusted supply chains. Secretary of DoE Orders banished one or another product from one or another region of the world. The Secretary DHS also issued restriction orders banning the use of certain suppliers' products from certain specific applications[3].

A Holistic Approach - Leveraging Nascent and Established Means

The International Society for Automation (ISA) BPS Working Group (ISA BPS WG) recommends the following four, inter-related projects in response to previous EOs, and department level procurement restrictions. On their own, each of these four projects brings significant improvements to the Supply Chain Risk Management (SCRM) processes employed by AOOs, global ICS/OT suppliers, and regulators. Collectively implemented, as a holistic approach, these four projects offer a synergistic amplification of improvements.

The bulletized list below provides an outline and overview, that is then followed by a somewhat more thorough description of each project:

- **Enabling Regulatory frameworks for Nuclear and BPS AOOs – Regs and Stds facing the AOO**
    a. Nuclear Power operation - NRC regulations in Title 10 of the Uniform Code of Federal Regulations.[4]
    b. Bulk Power System Standards - FERC/NERC Standards, Section 215 of the FFPA.[5]
    c. Emphasis
        1. NRC regulations - focused on <u>safe</u> operation of Nuclear Power.
        2. FERC/NERC standards - focused on the <u>reliable</u> operation of the BPS.
- **Enabling manufacturing standards for suppliers (goods and services) – Stds facing the suppliers**
    a. The ISA/IEC 62443 series for manufacturers, integrators, and products
    b. NIST Cybersecurity Framework and Special Publications 800-53, 800-62
    c. Emphasis
        1. Manufacturers are already adopting 62443 standards
        2. Cert bodies, certifying product, integration provider compliance, and similar activities.
- **Acquisition Resource Center (ARC) DoE and Others – connects the supply chain to consumer chain**
    a. Represents a "Node" within the Attestation Ecosystem (below)
    b. DOE ARC, required for certain acquisitions, based on existing NSA/DOD ARC
    c. A web-based portal - customers establish requirements and suppliers communicate configuration and other options.
    d. Suppliers Attestation Chain is tagged to Customer requirements and a Cryptologic Token (SCRM Token) is created and immutably attached to the supplier/customer transaction.
    e. Other product standards, such as ASME, Environmental, Mil-Specs, etc. and other codes are included, and sealed to the transaction via the SCRM Token.
- **Attestation Ecosystem – Enables transparent, secure, immutable transactions via nodes/channels**
    a. Nodes are implemented for each of the different parts of the design-build, procure-integrate-satisfy ARC customer requirements (including the DOE ARC itself)

[3] See banishment orders for PhishMe, Emerson EMS system with the Kaspersky security appliance, and others.
[4] NRC Regulations - https://www.nrc.gov/reactors.html
[5] FERC/NERC and the ERO - https://www.law.cornell.edu/uscode/text/16/824o

b. Channels are how supply elements transact, encapsulated SCRM Tokens to Smart Contracts.
c. This is an application of Blockchain technology and other advanced cryptologic methods.

The Four Projects in More Detail

I. Regulatory frameworks for asset owners and operators (AOOs) – Facing the AOO

Develop a Notice of Proposed Rule Making (NOPR).

The NOPR, recommended in this pathways approach, would start the Administrative Procedures Act controlled rulemaking process[6]. The NOPR process, an open process that requests stakeholder input, and results in a set of changes to NRC, and FERC/NERC regulations and Standards. These changes would enable full implementation of the technical recommendations of the Four Pathways approach.

As part of the NOPR processes certain desirable features of the new Rule are defined as goals of the NOPR. These desirable characteristics are naturally understood differently by different stakeholder' communities.

On such desirable characteristic of a proposed new rule would require the use of an ARC by all Asset Owners and Operators (AOO) for the acquisition of digital devices or services intended for use within certain critical systems. Criticality also being somewhat subjective. A common understanding of Critical-System could be systems in the BPS related to a Section 9 facility, DCEI, NERC Critical, or Nuclear Safety, etc.[7]. For devices related to these critical elements subject certain portions of NRC (Title 10) or FERC/NERC (FPA Section 215) regulations and standards could require use of an ARC. The appropriate enabling changes to Title 10CFR (NRC) and Standards from FERC/NERC's reliability standards will provide the necessary regulatory underpinnings for the various criticality of the CIKR.

The FERC/NERC and NRC regulatory authority will have the ability to query the DOE ARC and some of the other Attestation Channels and Nodes (e.g., NRC and FERC/NERC provided regulatory agency Nodes) about acquisitions or utilization of specific devices of concern.

> NOTE: The Attestation Ecosystem is further described below. At a superficial level, the Attestation Ecosystem contains Nodes, or portals, and Channels, or pathways of communications. Both a commercial provider and an open-source solution are available.[8]

NOPR attributes:

a) Should require use of the DOE ARC.
b) Require use of an Attestation Ecosystem (see another project).
c) Appropriate sections of the NRC regulations (10CFR) and FERC/NERC standards (CIP 013) provide necessary regulatory underpinnings for CIKR critical digital systems, such as DCEI etc.
d) The NOPR should stress regulatory support for an incentives approach.

[6] APA - The Administrative Procedure Act (APA) governs the process by which federal agencies develop and issue regulations

[7] Section 9 https://www.cisa.gov/publication/support-critical-infrastructure-greatest-risk-section-9-report-summary , Defense Critical Electric Infrastructure (DCEI) - https://www.energy.gov/sites/prod/files/2020/10/f79/OE%20DCEI%20Strategy%20for%20EAC%2010.14.20%20FINAL.pdf, NERC Critical - https://www.nerc.com/pa/Stand/CIP0024RD/Critcal%20Cyber%20Asset_approved%20by%20CIPCI%20and%20SC%20for%20Posting%20with%20CIP-002-1,%20CIP-002-2,%20CIP-002-3.pdf , Nuclear Safety NRC - https://en.wikipedia.org/wiki/Nuclear_Regulatory_Commission

[8] Fortress Security - https://fortressinfosec.com/solutions/ , https://www.cs2ai.org/post/the-time-has-come-to-automate-supply-chain-security

e) The NRC and FERC/NERC should coordinate with DOE on NOPR development.
Nuclear Sector Coordinating Council (NSCC) and Electricity Sector Coordinating Council (ESCC) should participate in the draft NOPR process as permissible, before release

Actions in addition to NOPR:

Implement Secretariat-level projects to improve or establish

a) DOE Acquisition Resource Center (ARC)
b) Attestation ecosystem for acquisition-related activities. The ecosystem provides the transparency and accountability components of the BPS SCRM. (See discussion on Attestation Ecosystem below)

II. Standards-based regulatory framework for the suppliers – Facing the Suppliers and Integrators

Widely adopted standards give the entire community – AOOs (buyers), Suppliers (sellers) and regulators – a common language, as well as a minimum acceptable baseline, with gradations above the baseline to protect against adversaries with higher levels of sophistication and resources. ISA/IEC 62443 is a suite of standards that addresses the entire automation lifecycle, from product design/development including risk assessment, through deployment and operations by the asset owners, and finally, through retirement. ISA/IEC 62443 component and systems certifications have been in use since 2010 and address the automation security at four levels of threat actor capability, including at the top, nation-state adversaries.

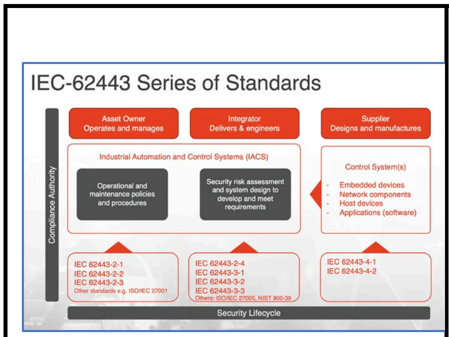
The standards are horizontally applicable across sectors including power, smart buildings/cities, industrial automation, medical, shipping, ONG, pipelines, transportation, and others. They have been adopted by many international governments with new jurisdictions such as the EU processing them into regulatory language. Existing assessment programs can be used in conjunction with advanced testing and analysis for key components by the US national labs, including DOE's CyTRICS program centered at the Idaho National Lab.

Already widely embraced by the supplier community, for efficiency, global companies desire to credential their products to a single global standard since most are selling into international markets, each with trading requirements that include cybersecurity capabilities.

Built on existing private sector standards-based cybersecurity assurance programs. For example, the International Society of Automation has been developing a comprehensive set of international standards purpose-built for automation and control technology. This is a family of standards with 15 key sections.

The ISA/IEC 62443 standards address the entire automation lifecycle, from product design/development including risk assessment, through deployment and operations by the asset owners, and finally, through retirement. ISA/IEC 62443 automation component and systems certifications have been operational since 2010 and address the mainstream automation security at four levels of risk, including nation-state adversaries.

The following three images provide an overview of the standards most applicable to the AOOs, as well as the ones that define requirements for suppliers.



IEC-62443 Series of Standards

Asset Owner
Operates and manages

Integrator
Delivers & engineers

Supplier
Designs and manufactures

Compliance Authority

Industrial Automation and Control Systems (IACS)

Operational and maintenance policies and procedures

Security risk assessment and system design to develop and meet requirements

Control System(s)

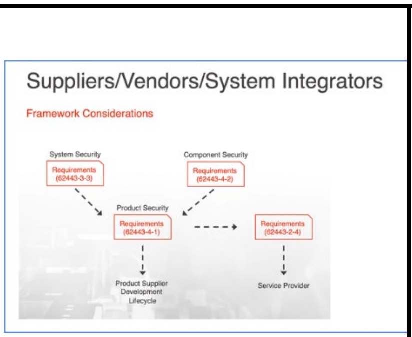
- Embedded devices
- Network components
- Host devices
- Applications (software)

IEC 62443-2-1
IEC 62443-2-2
IEC 62443-2-3
Other standards e.g. ISO/IEC 27001

IEC 62443-2-4
IEC 62443-3-1
IEC 62443-3-2
IEC 62443-3-3
Others: ISO/IEC 27005, NIST 800-39

IEC 62443-4-1
IEC 62443-4-2

Security Lifecycle



Suppliers/Vendors/System Integrators

Framework Considerations

System Security
Requirements (62443-3-3)

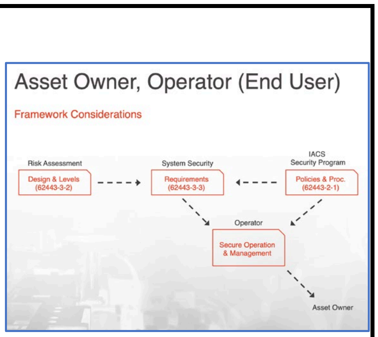
Component Security
Requirements (62443-4-2)

Product Security
Requirements (62443-4-1)

Requirements (62443-2-4)

Product Supplier Development Lifecycle

Service Provider



Asset Owner, Operator (End User)

Framework Considerations

Risk Assessment
Design & Levels (62443-3-2)

System Security
Requirements (62443-3-3)

IACS Security Program
Policies & Proc. (62443-2-1)

Operator
Secure Operation & Management

Asset Owner

The standards are also horizontally applicable across sectors including power, smart buildings/cities, industrial automation, medical, shipping, O&G, pipelines, transportation, and others. They have been adopted by many international governments with new jurisdictions such as the EU processing them into regulatory language.

The existing assessment programs can be used in conjunction with advanced testing and analysis for key components by the US national labs. I attached three documents which describe the ISA/IEC 62443 standards and one US based certification scheme (ISASecure). There are already over 15 certification bodies that are assessing to the 62443 standards, including 10 in the ISASecure program alone.

The allure of using international standards is support already demonstrated by the supplier community. These global companies desire to credential their products to a single global standard since most are selling into international markets; each with trading requirements that include cybersecurity capabilities. Most of the major suppliers are already certifying to ISA/IEC 62443.

III. DOE’s Acquisition Resource Centers (ARCs)

Procurement professionals need a way to set clearly defined performance and security requirements for the systems they buy and must be able to trust that the products delivered fully comply with the standards asserted by the manufacturer. They must also have assurance that for the products acquired, that the hardware, software, and firmware have not been tampered with or otherwise altered in transit. NSA maintains an ARC that is used for DoD and Intelligence Community purchasing, and it may serve as an excellent model for DOE as it modifies its own ARC for the organizations in its jusisdiction: the national labs, Power Marketing Administrations (PMAs), other DOE sites, the DOE headquarters in DC and other offices.

A secure DOE Acquisition Resource Center (ARC) will serve as the central point of access for all acquisitions of technology & services related to supporting and operating DCEI. The DOE ARC is where AOO and supplier procurement and engineering collaboration takes place.

The proposed DOE ARC can expand upon present DOE acquisition resource portals or redeploy the ARC portal like the one in use in the IC today. Ideally, this ARC creation, application, and evaluation will include input from suppliers/vendors and AOOs. The user community's involvement will ensure the adoption of the completed ARC by all relevant BPS stakeholders.

a) The proposed DOE ARC connects suppliers, asset owners and operators, federal agencies, and the Intelligence Community.
b) The ARC provides a secure central point of access for acquisition-related activities. This includes both existing vendor products as well as new product offerings. The assignment of a cryptologic attestation (SCRM Token – See glossary) to the procurement details being central to the ARC processes.
c) The ARC provides access to procurement engineering resources and facilitates collaboration among the supplier and AOO procurement engineering communities.
d) DOE can either modify its present acquisition portals or redeploy either the DOD or NSA ARC portal.
e) Modifications to the selected ARC will ensure use of the Block-Chain Cryptological Tokens (SCRM Tokens – see glossary) as used in the Attestation Ecosystem.
f) Ideally, ARC creation, application, and evaluation will include input from suppliers/vendors, the AOOs and various Doe, NRC, and FERC/NERC individuals. The stakeholder’s involvement will ensure the adoption of the completed ARC by all relevant BPS stakeholders.

IV. Attestation Ecosystem

At present, detailed BPS asset information, (e.g., hardware, software, firmware) is distributed across a multitude of systems in various formats. This information includes the sources of assets and materials, new software content, revisions to legacy software, custody, certification, known vulnerabilities, threat intelligence, and other system and component attributes. Supply chain risks are compounded by the inability of appropriate parties to access this information in a timely manner, if at all.

A secure and unified attestation-sharing ecosystem will provide DOE and AOOs timely access to actionable information and transparency throughout the entirety of the supply chain. Here are a few more details

An attestation ecosystem is a web of channels and nodes that provides the Transparency and the Accountability components of the BPS SCRM. Leveraging blockchain technology, it enables secure communication and information exchange among nodes connected by channels:

- Nodes -- for different parts of the Design-Build, Procure-integrate-satisfy Customer requirements
- Channels -- where supply elements transact – travel through – the "Crypto Coin" of a component of supply.

The use of cryptologic tokens (SCRM Tokens[9]), associated with the activities in different parts of the supply chain manufacturing processes provides the immutable Attestation elements for the accountability component of the Transparent and Accountable recommendations.

The relationships between the various manufacturing steps, or between manufacturer and customer, are handled through channels. These channels enforce either manufacturing rules, used between various manufacturing stages, or customer requirements defined within procurement instruments called purchase orders or even Smart-Contracts. These controlled relationships between various Nodes of the ecosystem are the Channels part of the ecosystem.

The various portals, the supplier portals (and Databases), the customer portals (and Databases), the modified DoE ARC (and associated resources), are the Nodes of the attestation ecosystems' Nodes and Channels. The digital procurement documents, Smart Contracts and such are securely passed throughout the procurement activities by the Channels established between various Nodes.

These manufacturers Nodes are where the cryptologic SCRM Tokens are logically fixed to the suppliers document stream as a product moves through its manufacturing processes. As the process unfolds additional blocks of the SCRM tokens are applied. The various Nodes, Portals or ARCs communicate with each other through various channels which ensure that the details of the devices and the attestation elements of the SCRM Tokens are managed between the various Nodes.

The use of controlled channels for communicating the manufacturing process details (Digital Bills of materials) and the locking of accountability (Attestation) at various phases in the product manufacturing lifecycle are the manufacturing Attestation Ecosystem.

[9] Use of Blockchain cryptologic techniques involving the Hash of a present manufacturing process document such as a BOM, and the "chaining" of this Hash to the processes before the present process in the manufacturing sequence. This method will build later steps, either the software "Build" process, or the component integration, assembly steps into the collecting SCRM Token.

As the supplier-to-customer acquisition process moves forward out of the Manufacturing processes and into the customer procurement processes, the DoE ARC provides a critical accountability check. The Requirement for use of the DoE ARC to finalize an acquisition for certain elements of CIKR resources allows for addition of DoE generated SCRM Tokens that would attest to suitability vis-a-vi USG requirements. These requirements at present are found in various Executive Orders, Procurement Restriction Orders, and or regulatory requirements. These elements of attestation may include items such as attesting to FOCI status (from Supplier), possible country of origin information (from Digital BOM), regulatory elements or requirements (From a Regulatory agency e.g., NRC FERC/NERC), and customer Term and Conditions (part of a Smart-Contract).

These steps, controlled by the DoE ARC portal, provide the relationship between the SCRM Tokens the supplier produced during product manufacturing, the controls required by various regulatory agencies, and the specific requirements of the Customer. The Nodes that apply the SCRM Tokens, the channels that control relationships and transport BOMs and SCRM Tokens comprise the ecosystem.

At present asset information, such as hardware or software bills of materials (BOM), is distributed in different systems and exists in different formats across the supply chain. This information includes the sources of assets and materials, new software content, a revision to legacy software, custody, certification, known vulnerability, threat intelligence, and other systems’ and components' attributes. Supply chain risks occur due to the inability of competent parties to access this information in a manner appropriate for the consequences. A consistent attestation-sharing ecosystem will provide Suppliers, DOE, AOOs, and regulators, actionable access to this information and transparency throughout the entirety of the supply chain.

a) Attestation Nodes currently under development will provide transparency throughout the entirety of the supply chain.
b) From global sources of materials to the development of new software to the revision of legacy software, often decades-old, the integration of an attestation ecosystem provides inherent transparency.
c) Attestation Channels are repositories governed by policies.
d) Channel Policies are enforced by Attestation Nodes, operated by or on behalf of supply chain actors.
e) Attestation Channels are created and used by SCRM stakeholders during supply chain-related activities.
f) Information sources such as suppliers, researchers, or AOOs populate Channels with attestations regarding content, origin, custody, and other assets' attributes.

Networks of Attestation Channels allow the resolution of concerns regarding the origin and handling of sub-assemblies, software, and integrated assemblies that may arise throughout the procurement and usage life cycle. The issues of concern can be identified specific to the manufacturing step where the concern arises. Having identified the origin of the concern the supplier is now able to review modifications to their manufacturing process to resolve the USG concern. This is not possible in the present supply chain.

Respectively Submitted:

Tim Roxey

To Join the ISA BPS Working Group	For technical questions regarding this document or its content
Andre Ristaino Managing Director, Global Alliances and Consortia International Society of Automation EU Office: +31 (0)6 33609357 US Office: +1 919-990-9222 Mobile Ph: +1 919-323-7660 aristaino@isa.org	Tim Roxey Scubanuke@gmail.com timroxey@comcast.net 410 474 9240

Acronyms and Glossary

AI/ML	Artificial Intelligence / Machine Learning
Airbox	Situational Awareness Tool from Gates Defensive Systems
AOO	Asset Owners and Operators
ARC	Acquisition Resource Center
BPS	Bulk Power System
CCE	Consequence-driven Cyber-informed Engineering
CMSCC	Critical Manufacturing Sector Coordinating Council
CyTRICS	Cyber Testing for Resilient Industrial Control System program (CyTRICS). CyTRICS enables DOE to evaluate software and firmware in energy sector equipment to identify and mitigate cybersecurity vulnerabilities in the supply chain, helping to ensure the integrity and reliability of critical system components nationwide.
DBoM	Digital Bills of Material
DBT	Design Based Threat
DCEI	Defense Critical Electric Infrastructure
E-ISAC	Electricity Information Sharing and Analysis Center
ENERGIZER system	
ESCC	Electric Sector Coordinating Council
FAST Act (DOE)	Fixing America's Surface Transportation Act- Section 215A
FOCI	Foreign Owned Controlled Influenced
IC	Intelligence Community
INL	Idaho National Labs
ISA	International society of Automation
Kill Chain	The Intelligence Driven Defense® model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete to achieve their objective.
MnA	Made in America
NETL	National Energy Technology Lab
Nodes and Channels	Attestation Channels ??
NOPR	Notice of Proposed Rulemaking
OMB	Office of Management and Budget
ONGSCC	Oil and Natural Gas Sector Coordinating Council
PMA	Power Marketing Administrations
SCRM	Supply Chain Risk Management
Tearline Report	Report that has sources and methods redacted
TLP	Traffic Light Protocol-defines information sharing policies