Revision ID: 0
Effective Date: 8/15/2019

Plan

Industrial Control System Cyber Security Plan Template

ORIGINAL

The ORIGINA National Lab is a U.S. Department of Energy National Laboratory operated by ACME Energy Alliance

Table of Contents

Mission/Objective /Purpose/Scope/Summary

Mission Example-INL Cyber Security Incident Response Plan

(INL-CyberSecurityIncidentResponsePlan, 2019)

Mission

The mission of the Idaho National Laboratory (INL) Cyber Security Incident Response Team (CSIRT) is to minimize disruption, downtime, and data loss of laboratory missions during times of cybersecurity-related attack.

Objective Example – State of Maryland IT Incident Management Plan

(State-of-Maryland-IT-Department-Security-Incident-Management-Plan, 2017)

Objective

The objective of this plan is to identify the policies, services, procedures, and requirements that help provide stable, effective incident management for an agency, and to help meet incident-management requirements in accordance with the Maryland *DoIT Incident Response Policy*.

Main objectives include:

- Establish the organizational obligations for monitoring, reporting, and responding to cyber incidents, including roles and responsibilities for incident reporting and handling
- Identify data under agency ownership that must be protected or may require special reporting if compromised
- Identify the persons responsible for cybersecurity within the agency and to provide specific contact information
- Outline steps to preserve incident data when security incidents are discovered
- To identify security reporting for the agency

Purpose Example - Unclassified INL Cyber Security Plan

(INL-UnclassifiedCyberSecurityProcedure, 2019)

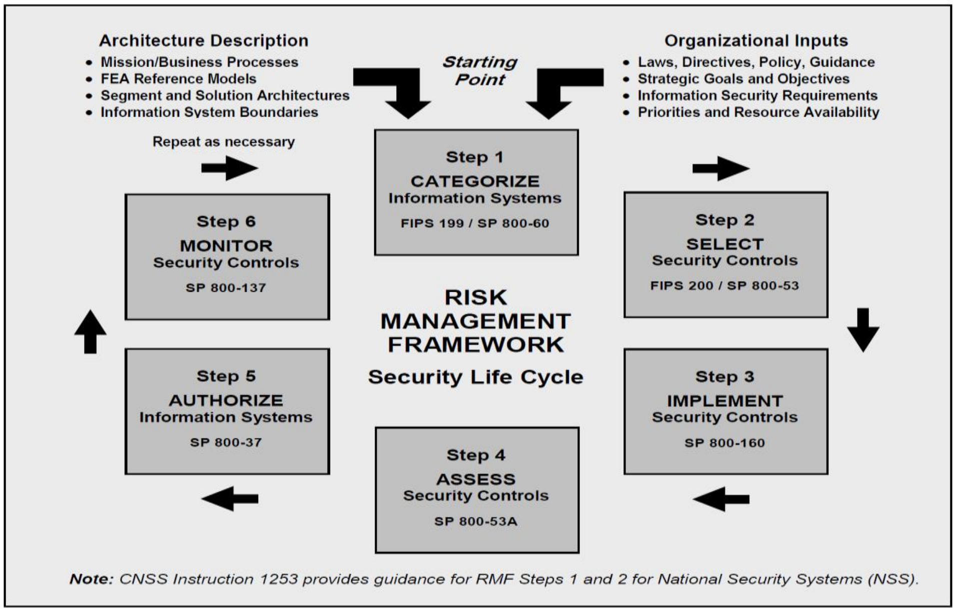
Purpose

This procedure documents the processes and activities required to protect the unclassified computing resources of Idaho National Laboratory (INL) unclassified *information systems* (see def.) in accordance with Department of Energy (DOE) Order 205.1B, “Department of Energy Cyber Security Program,” and “Energy Program’s Implementation Plan for the Departments Risk Management Approach” (RMA IP).

This graded approach is implemented at the system and *enclave* (see def.) level by utilizing appropriate baselines for security controls as defined by Federal Information Processing Standard (FIPS) Publication 199, “Standards for Security Categorization for Federal Information and Information Systems,” and FIPS Publication 200, “Minimum Security Requirements for Federal Information and Information Systems.” Furthermore, this approach is also consistent with guidelines from National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations.”

INL Cyber Security implements a Risk Management Framework (RMF) as the primary means for addressing risk. Cyber Security’s Risk Management Approach (RMA) employs a mission-focused

enterprise-wide method to securing information and information systems. The risk management processes cover the entire risk management lifecycle, providing a flexible process for cybersecurity risk management commensurate with mission needs.
The RMA, as characterized in Figure 1, consists of the following six phases of the authorization lifecycle:


Architecture Description
Mission/Business Processes
FEA Reference Models
Segment and Solution Architectures
Information System Boundaries
Starting Point
Organizational Inputs
Laws, Directives, Policy, Guidance
Strategic Goals and Objectives
Information Security Requirements
Priorities and Resource Availability
Repeat as necessary
Step 1 CATEGORIZE Information Systems FIPS 199 / SP 800-60
Step 2 SELECT Security Controls FIPS 200 / SP 800-53
Step 3 IMPLEMENT Security Controls SP 800-160
Step 4 ASSESS Security Controls SP 800-53A
Step 5 AUTHORIZE Information Systems SP 800-37
Step 6 MONITOR Security Controls SP 800-137
RISK MANAGEMENT FRAMEWORK
Security Life Cycle
Note: CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).

1. Categorize the information system based on a FIPS Publication 199 impact assessment.

2. Select the applicable security control baseline based on the results of the security categorization and apply tailoring guidance (including the potential use of overlays).

3. Implement the security controls and document the design, development, and implementation details for the controls.

4. Assess the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

5. Authorize information system operations based on a determination of risk to organizational operations and assets, individuals, other organizations, and the nation resulting from the operation and use of information systems and the decision that this risk is acceptable.
6. Monitor the security controls in the information system and environment of an operation on an ongoing basis to determine control effectiveness, changes to the system/environment, and compliance to legislation, Executive Orders, directives, policies, regulations, and standards.

Scope Example – National Rural Electric Cooperative Association

(NRECAGuidetoDevelopingaCyberSecurityandRiskMitigationPlan, 2011)

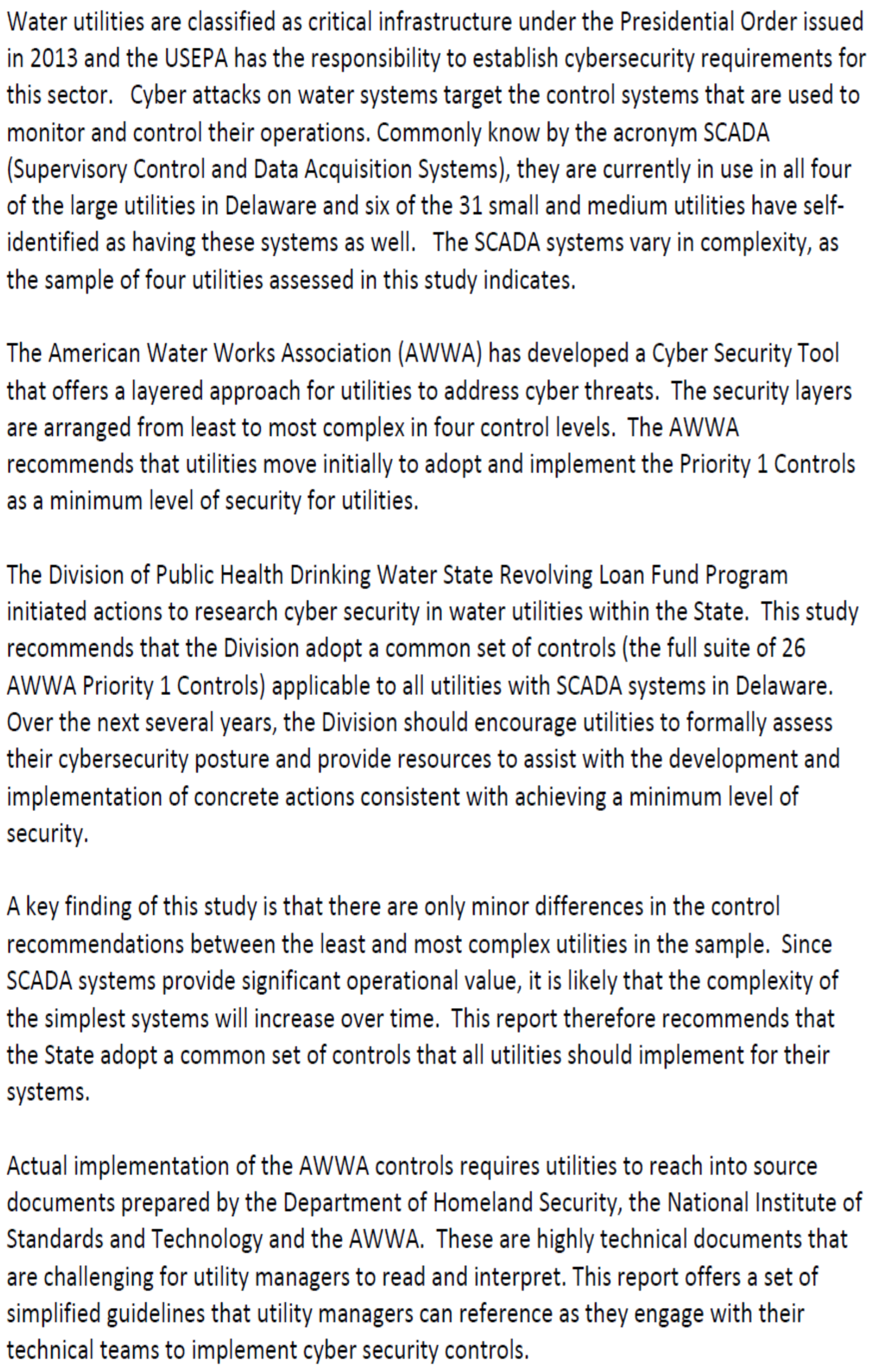
Scope

This document focuses on cyber security controls that an organization should have in place to meet the security challenges introduced by the smart grid.

Summary Example - American Water Works Association

(AmericanWaterWorksAssociationCyberSecurityAssessementAndRecommendedApproach, 2016)

Executive Summary



Water utilities are classified as critical infrastructure under the Presidential Order issued in 2013 and the USEPA has the responsibility to establish cybersecurity requirements for this sector. Cyber attacks on water systems target the control systems that are used to monitor and control their operations. Commonly know by the acronym SCADA (Supervisory Control and Data Acquisition Systems), they are currently in use in all four of the large utilities in Delaware and six of the 31 small and medium utilities have self-identified as having these systems as well. The SCADA systems vary in complexity, as the sample of four utilities assessed in this study indicates.

The American Water Works Association (AWWA) has developed a Cyber Security Tool that offers a layered approach for utilities to address cyber threats. The security layers are arranged from least to most complex in four control levels. The AWWA recommends that utilities move initially to adopt and implement the Priority 1 Controls as a minimum level of security for utilities.

The Division of Public Health Drinking Water State Revolving Loan Fund Program initiated actions to research cyber security in water utilities within the State. This study recommends that the Division adopt a common set of controls (the full suite of 26 AWWA Priority 1 Controls) applicable to all utilities with SCADA systems in Delaware. Over the next several years, the Division should encourage utilities to formally assess their cybersecurity posture and provide resources to assist with the development and implementation of concrete actions consistent with achieving a minimum level of security.

A key finding of this study is that there are only minor differences in the control recommendations between the least and most complex utilities in the sample. Since SCADA systems provide significant operational value, it is likely that the complexity of the simplest systems will increase over time. This report therefore recommends that the State adopt a common set of controls that all utilities should implement for their systems.

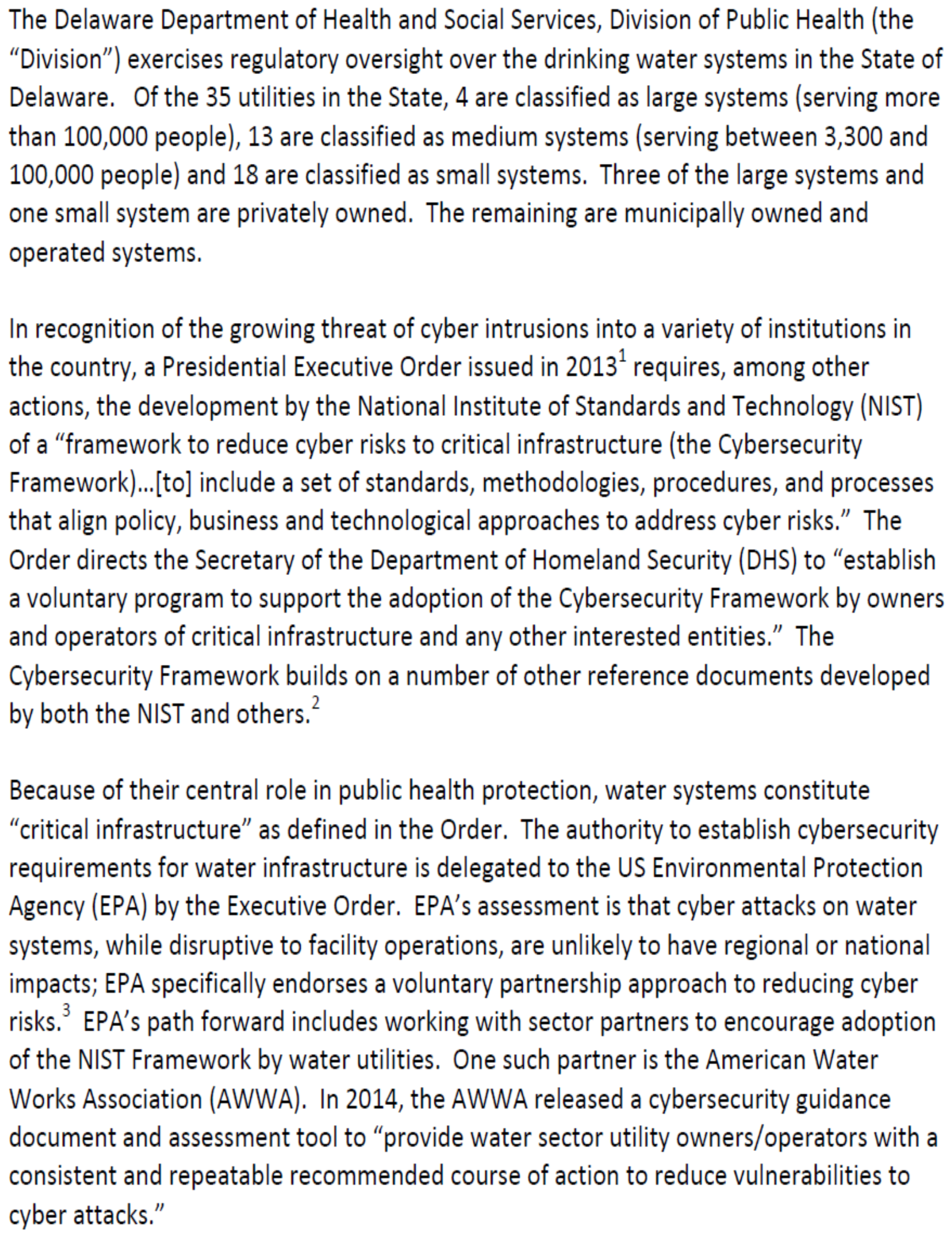
Actual implementation of the AWWA controls requires utilities to reach into source documents prepared by the Department of Homeland Security, the National Institute of Standards and Technology and the AWWA. These are highly technical documents that are challenging for utility managers to read and interpret. This report offers a set of simplified guidelines that utility managers can reference as they engage with their technical teams to implement cyber security controls.

Background

Background Example - American Water Works Association

(AmericanWaterWorksAssociationCyberSecurityAssessementAndRecommendedApproach, 2016)

Background



The Delaware Department of Health and Social Services, Division of Public Health (the "Division") exercises regulatory oversight over the drinking water systems in the State of Delaware. Of the 35 utilities in the State, 4 are classified as large systems (serving more than 100,000 people), 13 are classified as medium systems (serving between 3,300 and 100,000 people) and 18 are classified as small systems. Three of the large systems and one small system are privately owned. The remaining are municipally owned and operated systems.

In recognition of the growing threat of cyber intrusions into a variety of institutions in the country, a Presidential Executive Order issued in 2013[1] requires, among other actions, the development by the National Institute of Standards and Technology (NIST) of a "framework to reduce cyber risks to critical infrastructure (the Cybersecurity Framework)…[to] include a set of standards, methodologies, procedures, and processes that align policy, business and technological approaches to address cyber risks." The Order directs the Secretary of the Department of Homeland Security (DHS) to "establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities." The Cybersecurity Framework builds on a number of other reference documents developed by both the NIST and others.[2]

Because of their central role in public health protection, water systems constitute "critical infrastructure" as defined in the Order. The authority to establish cybersecurity requirements for water infrastructure is delegated to the US Environmental Protection Agency (EPA) by the Executive Order. EPA's assessment is that cyber attacks on water systems, while disruptive to facility operations, are unlikely to have regional or national impacts; EPA specifically endorses a voluntary partnership approach to reducing cyber risks.[3] EPA's path forward includes working with sector partners to encourage adoption of the NIST Framework by water utilities. One such partner is the American Water Works Association (AWWA). In 2014, the AWWA released a cybersecurity guidance document and assessment tool to "provide water sector utility owners/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyber attacks."

Outcomes/Applicability

Outcomes Example – INL Cyber Security Program Operations Plan

(INL-CyberSecurityProgramOperationsPlan, 2018)

Outcomes

1. Maintain and implement the Under Secretary of Energy RMA in accordance with the DOE requirement.
2. Maintain up-to-date certification and accreditation packages for classified and unclassified computing systems in accordance with DOE requirements. All national security systems must be recertified at least every three years in accordance with DOE requirements.
3. Maintain up-to-date cyber contractor assurance system to measure performance and process improvement.
4. Complete cyber security life-cycle hardware/software upgrades and replacements on classified and unclassified systems consistent with cyber security life-cycle management planning and schedules.
5. Re-certify and accredit the Infrastructure and General Purpose unclassified systems from low to moderate enclave by March 20xx.
6. Implement first phase of an Industrial Control Systems assurance program by September 20xx.
7. Implement an enhanced vulnerability management program for INL unclassified systems by September 20xx.
8. Complete comprehensive review of reaccreditation package for re-certification and accreditation of the SMC NSS by September 20xx.
9. Continue to implement the Identity, Credential, and Access Management project in accordance with DOE requirements

Applicability Example –INL Unclassified Cyber Security Procedure

(INL-UnclassifiedCyberSecurityProcedure, 2019)

Applicability

This procedure applies to the staff of the Unclassified Security organization. The responsibilities of the identified performers are defined in Appendix B-Responsibilities.

Assumptions and Constraints

Example – INL Cyber Security Program Operations Plan

(INL-CyberSecurityProgramOperationsPlan, 2018)

Assumptions and Constraints

The following are **assumptions** upon which this plan is based:
1. Leadership fully authorizes the Cyber Security program to carry out its functions in order to achieve the stated outcomes.
2. Information about the cyber security status of any network, system, or application is always freely available to the Cyber Security program in order to assess risk.
3. All new technology deployments and changes to existing production deployments will be handled in a change management process whereby security-significant changes are identified and assessed with Cyber Security personnel before changes are made.

At development of this plan, the following **constraints** have been identified:
1. Authorization to Operate (ATO) of technology systems within the environment is granted by DOE-ID, which has the final authority per DOE Order 205.1b to accept risk. Cyber Security cannot override the decision of the Authorizing Official.
2. Monitoring of systems on a 24×7 basis is limited given the current number of personnel on the Cyber Operations team. Some system monitoring is performed 24×7, but that monitoring is a second-level control.
3. Organization-wide financial systems and schedules.

If any of the assumptions or constraints change, this plan needs to be reviewed for impacts.

Develop Cyber Security Defensive Strategy (i.e., defensive model)

Example: Develop Defensive Strategy –

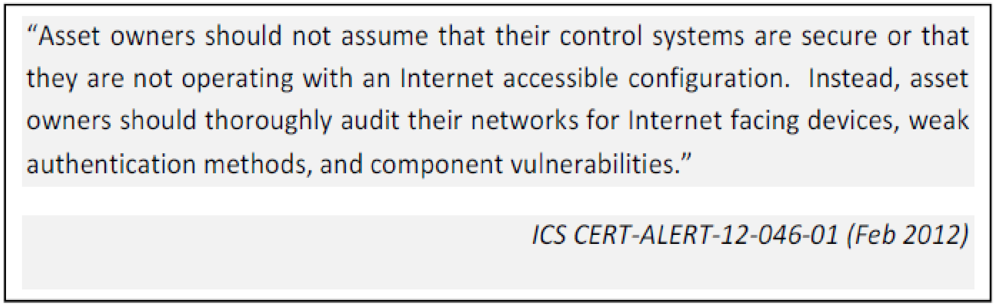
(United-States-Nuclear-Regulatory-Commission-Part73-Cyber-Security-Plan-Implementation-Schedule, 2018)

Develop an ICS Defensive Strategy model

Defensive Strategy (i.e., defensive model)	The Defensive Strategy expands upon the high level model in the Cyber Security Plan and requires assessment of existing site and corporate policies, comparison to new requirements, revisions as required, and communication to plant personnel. By the completion date, the following will be performed: • Documenting the defense-in-depth architecture and defensive strategy; • Revisions to existing defensive strategy policies will be implemented and communicated; and • Planning the implementation of the defense-in-depth architecture.
Implement cyber security defense-in-depth architecture	The implementation of communication barriers protects the most critical SSEP functions from remote attacks on our plant systems. Isolating the plant control systems from the Internet as well as from the corporate business systems is an important milestone in defending against external threats. [Recognizing the threat vectors associated with electronic access, the installation of hardware-based deterministic isolation devices will be prioritized.] While the deployment of the barriers is critical to protection from external cyber threats, it also prevents remote access to core monitoring and plant data systems for reactor engineers and other plant staff. This elimination of remote access to reactor core monitoring systems requires the development and execution of a detailed change management plan to ensure continued safe operation of the plants. Vendors may be required to develop software revisions to support the model. The modification will be developed, prioritized and scheduled. Since software must be updated on and data retrieved from isolated systems, a method of patching, updating and scanning isolated devices will be developed.

Example: Defense-in-Depth DOD ICS Handbook for ICS, 2012)

(Handbook-for-Self-Assessing_Security_Vulnerabilities&Risks_of_Industrial_Control_Systems_on_DOD_Installations, 2012)



"Asset owners should not assume that their control systems are secure or that they are not operating with an Internet accessible configuration. Instead, asset owners should thoroughly audit their networks for Internet facing devices, weak authentication methods, and component vulnerabilities."

ICS CERT-ALERT-12-046-01 (Feb 2012)

ICS Defense-in-Depth Cyber Security Actions

Define and defend perimeters. "Defense in depth" is an operative phrase often encountered. Strategic approaches include creating enclaves, segmentation, and establishing demilitarized zones (DMZ), typically using firewalls. NSA, DHS, and others recommend total isolation of ICS networks but that is not always possible or practical.

Where some connectivity is required, at least secure the points where connection can be made.

Control web access. Where Internet or NIPRNet connectivity is required limit access to the web by turning off unnecessary web services and ports, and consider using "white" and/or "black" lists of allowed/not allowed sites. (Note: Whitelisting is often preferred over blacklisting.)

Protect data. Encrypt mission-critical data in transmission and provide backups or other redundancies for data in stasis (files, databases, etc.). As a caveat, downstream data such as between a PLC and a field device cannot be encrypted.

Protect the operating system. Perimeter defense is a good start, but threat actors (insiders, for example) can find ways inside the perimeter. Use defensive tools34 (software) such as for intrusion detection. Implement and update virus-checking software (may need to do manually if not connected). Establish a patching protocol (typically requires testing off-line first). Enable audit logging, and review the logs frequently to detect anomalous (especially illegitimate) activity. Also, remove all services, programs, etc. not needed for operation of the ICS.

Manage installation of new assets. Ensure hardware and software factory default or contractor-enabled settings are changed. Do not allow anything that is connected/connectable, new or legacy, to be accessed using default passwords. Vendors prefer to maintain defaults especially on field devices (e.g., PLCs) for ease of maintenance access. Those same defaults typically are publically accessible, often published on vendor company web sites, and will be used by threat actors.

Disable every connection point not needed. Points include USB ports, wireless access points, Ethernet jacks, satellite receivers, modems, etc. Provide positive control over all remaining points, ensuring no "backdoor" exists. Even one unguarded USB port can provide a devastating threat vector. This point is demonstrated by the publically reported outcome of the Stuxnet infection of an Iranian nuclear processing facility's centrifuge control system.

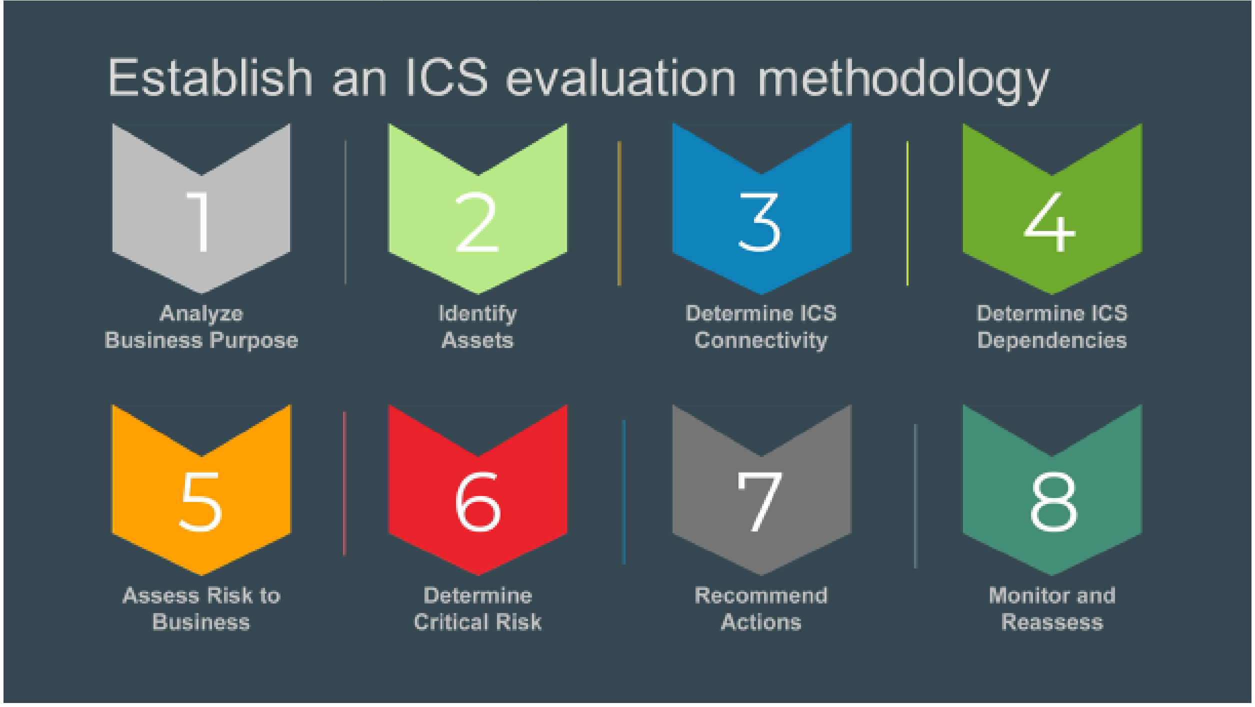
Control individual access to all elements. The operating system server and workstations are obvious control points but some field elements such as PLCs can (and do) have separate logons. There are a number of operational and tactical actions to take, selectively or collectively. Foremost is to require each individual to have a unique (unshared) logon ID and password.35 Policy should strictly prohibit shared passwords. Institute least-privilege and role-based access. Absolutely nothing should be accessible via "guest" or anonymous accounts, in spite of very plausible rationale for such given by vendors. Administrator privileges should be given to vendors only as required and then closely monitored.

Vulnerability and threat assessment

Example – ICS (Assessment) Evaluation of ICS Cyber Security Posture

(Handbook-for-Self-Assessing_Security_Vulnerabilities&Risks_of_Industrial_Control_Systems_on_DOD_Installations, 2012)

Establish process for ICS Cybersecurity Threats and Vulnerabilities



Establish an ICS evaluation methodology

1 Analyze Business Purpose

2 Identify Assets

3 Determine ICS Connectivity

4 Determine ICS Dependencies

5 Assess Risk to Business

6 Determine Critical Risk

7 Recommend Actions

8 Monitor and Reassess

Understand Uniqueness of Scanning IT vs. ICS environments

RA-5 ICS Supplemental Guidance: Vulnerability scanning and penetration testing are used with care on ICS networks to ensure that ICS functions are not adversely impacted by the scanning process. Production ICS may need to be taken offline, or replicated to the extent feasible, before scanning can be conducted. If ICS are taken offline for scanning, scans are scheduled to occur during planned ICS outages whenever possible. If vulnerability scanning tools are used on non-ICS networks, extra care is taken to ensure that they do not scan the ICS network. In situations where the organization cannot, for operational reasons, conduct vulnerability scanning on a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct scanning) in accordance with the general tailoring guidance.

(GuidetoIndustrialControlSystems(ICS)Security-Stouffer, 2015)

Define System and Criticality Levels; analyze and prioritize business/mission

Example – Define the Systems National Rural Electric Cooperative Association

(NRECAGuidetoDevelopingaCyberSecurityandRiskMitigationPlan, 2011)

Define the System

Careful system definitions are essential to the accuracy of vulnerability and risk assessments and to the selection of controls that will provide adequate assurances of cyber security. Not all systems require the same level of protection. The following are a few major elements of a system definition:
The logical and physical boundaries of the system within its environment:

- Which components and resources belong to the system?
- Which are external to the system?
- The system's mission and primary functions.
- The system's architecture (physical, logical, and security) and data flows.
- Details for interfaces and protocols.
- Types of information the system stores, uses, or transmits, and the sensitivity of each.
- Existing management, technical, operational, and physical security controls.

Example1: Determine System Criticality Level – New York State IT Security Plan Template

(New-York-State-Information-Security-plan-template-Defense-Counterintelligence-and-Security-Agency, 2018)

Define/Create a System Criticality Profile- Example 1

In the table below, record the System Criticality Profile of all systems and applications that are within the scope of this project. The criticality profile is qualitative with the possible choices being Mission Critical (MC), Mission Important (MI) and Mission Supportive (MS).

Table II-B-2: System Criticality Profile

System / Application Name	Criticality Level (MC/MI/MS)	Description

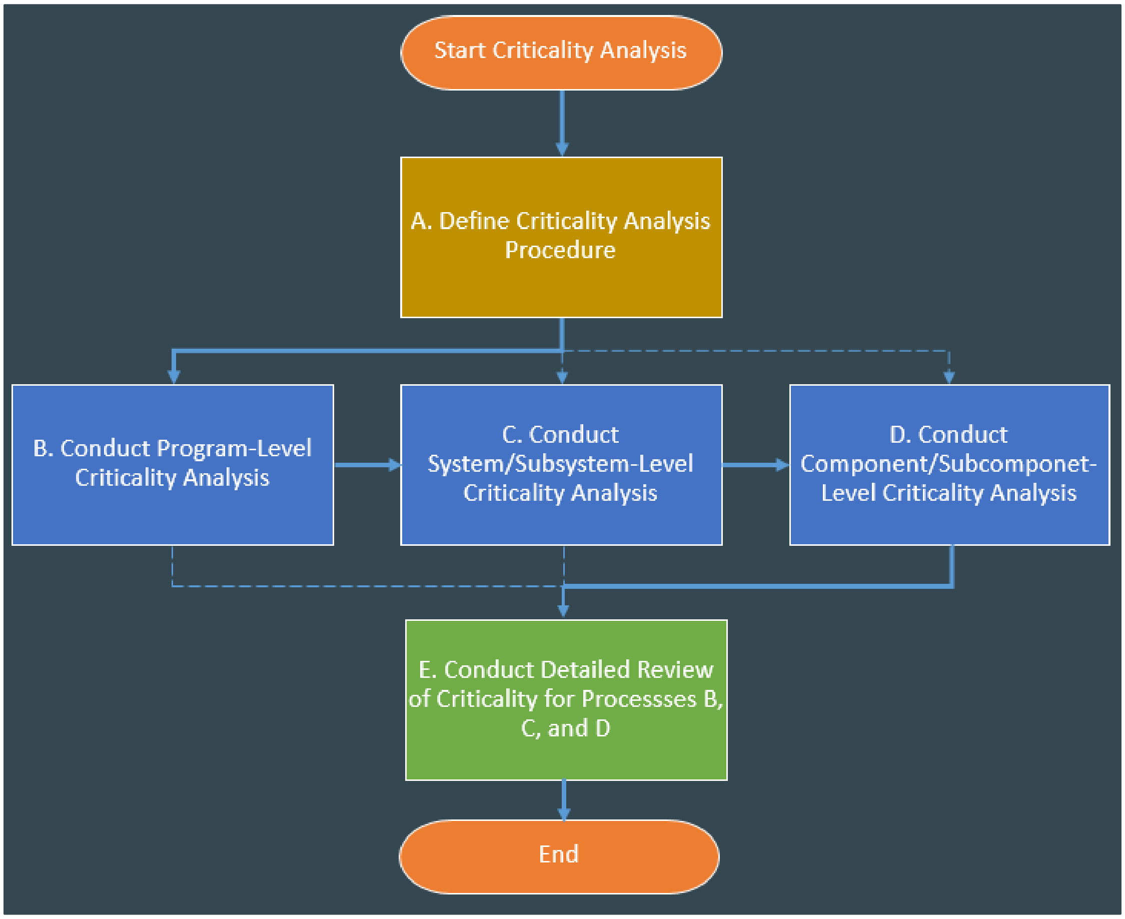
Definitions:

Mission Critical (MC) – Automated information resources whose failure would preclude the Agency from accomplishing its core business operations.
Mission Important (MI) – Automated information resources whose failure would not preclude the Agency from accomplishing core business processes in the short term, but would cause failure in the mid to long term (3 days to 1 month).
Mission Supportive (MS) – Automated information resources whose failure would not preclude the Agency from accomplishing core business operations in the short to long term (more than 1 month), but would have an impact on the effectiveness or efficiency of day-to-day operations.

Example2: Determine System Criticality Level – NIST Criticality Analysis Process Model

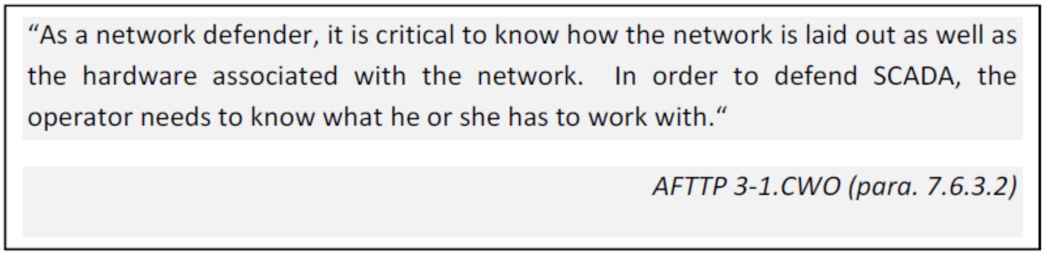
(NISTIR8179-Criticality-Analysis-Process-Model-Prioritizing-Systems-and-Components, 2017)

Define/Create a System Criticality Example 2


Start Criticality Analysis
A. Define Criticality Analysis Procedure
B. Conduct Program-Level Criticality Analysis
C. Conduct System/Subsystem-Level Criticality Analysis
D. Conduct Component/Subcomponet-Level Criticality Analysis
E. Conduct Detailed Review of Criticality for Processses B, C, and D
End

Example: Determine Business/Mission Criticality – ICS Handbook

Determine Business/Mission Criticality



> "As a network defender, it is critical to know how the network is laid out as well as the hardware associated with the network. In order to defend SCADA, the operator needs to know what he or she has to work with."
>
> *AFTTP 3-1.CWO (para. 7.6.3.2)*

Step 1. **Mission analysis**. For ICS defense, the task is to establish a baseline understanding among the stakeholders of the missions relative to the support infrastructure (both IT and

ICS). A key product of this first step is a prioritization of missions that can be linked to assets and then ICS dependencies. Key question: If I have to devote all of my very limited resources to protecting one mission, what would that be? Then the one after that?

Applying Mission Assurance Category (MAC) levels25 can be useful to this endeavor. Also included may be a review of Mission Essential Tasks (MET) 26 with reference to the Defense

Readiness Reporting System (DRRS). Mission analysis and decomposition, especially to a granularity useful to the rest of the steps, likely will not be a trivial process and may require significant commitment of the resource of time. A solid investment of time at this step will make the follow-on steps easier to accomplish.

Step 2. Identify assets. This includes not only direct mission assets (such as aircraft, tanks, ships, etc.) but more pointedly the infrastructure systems (such as fuels management and delivery) that support those. The key is to identify the thread from mission to asset to supporting infrastructure to ICS dependencies. This thread will reveal which ICS systems are more critical when it comes to applying security controls.

Step 3. Determine ICS connectivity. It is absolutely essential to identify every point of connectivity because the greatest vulnerability is at any point of connection. While NIPRNet connectivity may take top tier on the list, any connectivity—whether currently connected or could be connected later—must be identified. To leave even one potential connection undiscovered possibly is to leave the entire network vulnerable. Running a scan on the network elements will identify only what is connected and on at the moment of the scan. This is a key reason for conducting a physical inventory as well, setting eyes on any and every potential connection capability. A PLC may be inside a locked cabinet inside

a fenced compound with armed guards at a gate, but if it has an Ethernet port it is connectible (e.g., for vendor maintenance) and therefore, is a potential risk.

Step 4. Determine ICS dependencies. Which missions and their supporting infrastructure are dependent on a properly functioning control system? Are multiple control systems involved (as in the earlier example of traffic control, emergency systems, and fuels delivery)? This step also requires technical network mapping typically coupled with a physical inventory and an operational-level understanding of the missions.

Mapping Interdependencies, for an example methodology. A comprehensive approach to this must be followed with collaboration among representatives from at least the cyber, engineering, and mission operations communities.

Identify and classify critical cyber assets

Example - Data/information classification, marking

(Federal-Communications-Commission-Small-Biz-Cyber-Security-Planning-Guide, 2012)

Data/information classification/marking

Protecting data, like any other security challenge, is about creating layers of protection. The idea of layering security is simple: You cannot and should not rely on just one security mechanism – such as a password – to protect something sensitive. If that security mechanism fails, you have nothing left to protect you.

When it comes to data security, there are a number of key procedural and technical layers you should:

Inventory your data

We mentioned before the need to conduct a data inventory so you have a complete picture of all the data your business possesses or controls. It's essential to get a complete inventory, so you don't overlook some sensitive data that could be exposed.

Identify and protect your sensitive and valuable data

Data classification is one of the most important steps in data security. Not all data is created equal, and few businesses have the time or resources to provide maximum protection to all their data. That's why it's important to classify your data based on how sensitive or valuable it is – so that you know what your most sensitive data is, where it is and how well it's protected.

Common data classifications include:

> **HIGHLY CONFIDENTIAL**: This classification applies to the most sensitive business information that is intended strictly for use within your company. Its unauthorized disclosure could seriously and adversely impact your company, business partners, vendors and/or customers in the short and long term. It could include credit-card transaction data, customer names and addresses, card magnetic stripe contents, passwords and PINs, employee payroll files, Social Security numbers, patient information (if you're a healthcare business) and similar data.
>
> **SENSITIVE**: This classification applies to sensitive business information that is intended for use within your company, and information that you would consider to be private should be included in this classification. Examples include employee performance evaluations, internal audit reports, various financial reports, product designs, partnership agreements, marketing plans and email marketing lists.
>
> **INTERNAL USE ONLY**: This classification applies to sensitive information that is generally accessible by a wide audience and is intended for use only within your company. While its unauthorized disclosure to outsiders should be against policy and may be harmful, the unlawful disclosure of the information is not expected to impact your company, employees, business partners, vendors and the like.

Example System and data integrity

(Federal-Communications-Commission-Small-Biz-Cyber-Security-Planning-Guide, 2012)

Data handling/restrictions

Control access to your data

No matter what kind of data you have, you must control access to it. The more sensitive the data, the more restrictive the access. As a general rule, access to data should be on a need-to-know basis. Only individuals who have a specific need to access certain data should be allowed to do so.

Once you've classified your data, begin the process of assigning access privileges and rights – that means creating a list of who can access what data, under what circumstances, what they are and are not allowed to do with it and how they are required to protect it. As part of this process, a business should consider developing a straightforward plan and policy – a set of guidelines – about how each type of data should be handled and protected based on who needs access to it and the level of classification.

Secure your data

In addition to administrative safeguards that determine who has access to what data, technical safeguards are essential. The two primary safeguards for data are passwords and encryption.

Passwords implemented to protect your most sensitive data should be the strongest they can reasonably be. That means passwords that are random, complex and long (at least 10 characters), that are changed regularly and that are closely guarded by those who know them. Employee training on the basics of secure passwords and their importance is a must.

Passwords alone may not be sufficient to protect sensitive data. Businesses may want to consider two-factor authentication, which often combines a password with another verification method, such as a dynamic personal identification number, or PIN.

Some popular methods of two-factor identification include:

- Something the requestor individually knows as a secret, such as a password or a PIN.
- Something the requestor uniquely possesses, such as a passport, physical token or ID card.
- Something the requestor can uniquely provide as biometric data, such as a fingerprint or face geometry.

Another essential data protection technology is encryption. Encryption has been used to protect sensitive data and communications for decades, and today's encryption is very affordable, easy-to-use and highly effective in protecting data from prying eyes.

Encryption encodes or scrambles information to such an advanced degree that it is unreadable and unusable by anyone who does not have the proper key to unlock the data. The key is like a password, so it's very important that the key is properly protected at all times.

Encryption is affordable for even the smallest business, and some encryption software is free. You can use encryption to encrypt or protect an entire hard drive, a specific folder on a drive or just a single document. You can also use encryption to protect data on a USB or thumb drive and on any other removable media.

Because not all levels of encryption are created equal, businesses should consider using a data encryption method that is FIPS-certified (Federal Information Processing Standard), which means it has been certified for compliance with federal government security protocols.

Back up your data

Just as critical as protecting your data is backing it up. In the event that your data is stolen by thieves or hackers, or even erased accidentally by an employee, you will at least have a copy to fall back on.

Put a policy in place that specifies what data is backed up and how; how often it's backed up; who is responsible for creating backups; where and how the backups are stored; and who has access to those backups. Small businesses have lots of affordable backup options, whether it's backing up to an external drive in your office, or backing up automatically and online so that all your data is stored at a remote and secure data center. Remember, physical media such as a disc or drive used to store a data backup is vulnerable no matter where it is, so make sure you guard any backups stored in your office or off site and also make sure that your backup data storage systems are encrypted.

Assess Risk

Example-Identify and analyze the electronic security perimeter

(Federal-Communications-Commission-Small-Biz-Cyber-Security-Planning-Guide, 2012)

Network Security

Securing your company's network consists of: (1) identifying all devices and connections on the network; (2) setting boundaries between your company's systems and others; and (3) enforcing controls to ensure that unauthorized access, misuse, or denial-of-service events can be thwarted or rapidly contained and recovered from if they do occur.

Cyber Plan Action Items:

1. Secure internal network and cloud services

Your company's network should be separated from the public Internet by strong user authentication mechanisms and policy enforcement systems such as firewalls and web filtering proxies. Additional monitoring and security solutions, such as anti-virus software and intrusion detection systems, should also be employed to identify and stop malicious code or unauthorized access attempts.

Internal network

After identifying the boundary points on your company's network, each boundary should be evaluated to determine what types of security controls are necessary and how they can be best deployed. Border routers should be configured to only route traffic to and from your company's public IP addresses, firewalls should be deployed to restrict traffic only to and from the minimum set of necessary services, and intrusion prevention systems should be configured to monitor for suspicious activity crossing your network perimeter. In order to prevent bottlenecks, all security systems you deploy to your company's network perimeter should be capable of handling the bandwidth that your carrier provides.

Cloud based services

Carefully consult your terms of service with all cloud service providers to ensure that your company's information and activities are protected with the same degree of security you would intend to provide on your own. Request security and auditing from your cloud service providers as applicable to your company's needs and concerns.

Review and understand service level agreements, or SLAs, for system restoration and reconstitution time. You should also inquire about additional services a cloud service can provide. These services may include backup and restore services and encryption services, which may be very attractive to small businesses.

2. Develop strong password policies

Generally speaking, two-factor authentication methods, which require two types of evidence that you are who you claim to be, are safer than using just static passwords for authentication. One common example is a personal security token that displays changing passcodes to be used in conjunction with an established password. However, two-factor systems may not always be possible or practical for your company.

Password policies should encourage your employees to employ the strongest passwords possible without creating the need or temptation to reuse passwords or write them down. That means passwords that are random, complex and long (at least 10 characters), that are changed regularly, and that are closely guarded by those who know them.

3. Secure and encrypt your company's Wi-Fi

Wireless access control

Your company may choose to operate a Wireless Local Area Network (WLAN) for the use of customers, guests and visitors. If so, it is important that such a WLAN be kept separate from the main company network so that traffic from the public network cannot traverse the company's internal systems at any point.

Internal, non-public WLAN access should be restricted to specific devices and specific users to the greatest extent possible while meeting your company's business needs. Where the internal WLAN has less stringent access controls than your company's wired network, dual connections -- where a device is able to connect to both the wireless and wired networks simultaneously -- should be prohibited by technical controls on each such capable device (e.g., BIOS-level LAN/WLAN switch settings). All users should be given unique credentials with preset expiration dates to use when accessing the internal WLAN.

Wireless encryption

Due to demonstrable security flaws known to exist in older forms of wireless encryption, your company's internal WLAN should only employ Wi-Fi Protected Access 2 (WPA2) encryption.

4. Encrypt sensitive company data

Encryption should be employed to protect any data that your company considers sensitive, in addition to meeting applicable regulatory requirements on information safeguarding. Different encryption schemes are appropriate under different circumstances. However, applications that comply with the OpenPGP standard, such as PGP and GnuPG, provide a wide range of options for securing data on disk as well as in transit. If you choose to offer secure transactions via your company's website, consult with your service provider about available options for an SSL certificate for your site.

5. Regularly update all applications

All systems and software, including networking equipment, should be updated in a timely fashion as patches and firmware upgrades become available. Use automatic updating services whenever possible, especially for security systems such as anti-malware applications, web filtering tools and intrusion prevention systems.

6. Set safe web browsing rules

Your company's internal network should only be able to access those services and resources on the Internet that are essential to the business and the needs of your employees. Use the safe browsing features included with modern web browsing software and a web proxy to ensure that malicious or unauthorized sites cannot be accessed from your internal network.

7. If remote access is enabled, make sure it is secure

If your company needs to provide remote access to your company's internal network over the Internet, one popular and secure option is to employ a secure Virtual Private Network (VPN) system accompanied by strong two-factor authentication, using either hardware or software tokens.

8. Create Safe-Use Flash Drive Policy

Ensure employees never put any unknown flash drive or USBs into their computer. As the U.S. Chamber's *Internet Security Essentials for Business 2.0* states, small businesses should set a policy so that employees know they should never open a file from a flash drive they are not familiar with and should hold down the Shift key when inserting the flash drive to block malware.

Example: Wireless Security (WIDS)

(NIST-800-94-GuidetoIntrusionDetectionandPreventionSystems, 2007)

Wireless Security

A wireless IDPS monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity. The typical components in a wireless IDPS are the same as a network-based IDPS: consoles, database servers (optional), management servers, and sensors. However, unlike a network-based IDPS sensor, which can see all packets on the networks it monitors, a wireless IDPS sensor works by sampling traffic because it can only monitor a single channel at a time. The longer a single channel is monitored, the more likely it is that the sensor will miss malicious activity occurring on other channels. To avoid this, sensors typically change channels frequently, so that they can monitor each channel a few times per second. Wireless sensors are available in multiple forms. A dedicated sensor is a fixed or mobile device that performs wireless IDPS functions but does not pass network traffic from source to destination. The other wireless sensor forms are bundled with access points (AP) or wireless switches. Because dedicated sensors can focus on detection and do not need to carry wireless traffic, they typically offer stronger detection capabilities than wireless sensors bundled with access points or wireless switches. However, dedicated sensors are often more expensive to acquire, install, and maintain than bundled sensors because bundled sensors can be installed on existing hardware, whereas dedicated sensors involve additional hardware and software. Organizations should consider both security and cost when selecting wireless IDPS sensors. Wireless IDPS components are typically connected to each other through a wired network. Because there should already be a strictly controlled separation between the wireless and wired networks, using either a management network or a standard network should be acceptable for wireless IDPS components. Choosing sensor locations for a wireless IDPS deployment is a fundamentally different problem than choosing locations for any other type of IDPS sensor. If the organization uses wireless local area networks (WLAN), wireless sensors should be deployed so that they monitor the range of the WLANs. Many organizations also want to deploy sensors to monitor parts of their facilities where there should be no WLAN activity, as well as channels and bands that the organization's WLANs should not use. Other considerations for selecting sensor locations include physical security, sensor range, wired network connection availability, cost, and AP and wireless switch locations. Wireless IDPSs provide several types of security capabilities. Most can collect information on observed wireless devices and WLANs and perform extensive logging of event data. Wireless IDPSs can detect attacks, misconfigurations, and policy violations at the WLAN protocol level. Organizations should use wireless IDPS products that use a combination of detection techniques to achieve broader and more accurate detection. Examples of events detected by wireless IDPSs are unauthorized WLANs and WLAN devices, poorly secured WLAN devices, unusual usage patterns, the use of active wireless network scanners, denial of service attacks, and impersonation and man-in-the-middle attacks. Most wireless IDPS sensors can also identify the physical location of a detected threat by using triangulation. Compared to other forms of IDPS, wireless IDPS is generally more accurate; this is largely due to its limited scope (analyzing wireless networking protocols). Wireless IDPSs usually require some tuning 5-12 GUIDE TO INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS) and customization to improve their detection accuracy. The main effort is in specifying which WLANs, APs, and STAs are authorized, and in entering the policy characteristics into the wireless IDPS software. Besides reviewing tuning and customizations periodically to ensure that they are still accurate, administrators should also ensure that changes to building plans are incorporated occasionally. This is needed for accurate identification of the physical location of threats and accurate planning of sensor deployments. Although wireless IDPSs offer robust detection capabilities, they do have some significant limitations. Wireless IDPSs cannot detect certain types of attacks against wireless networks, such as attacks involving passive monitoring and offline processing of wireless traffic. Wireless IDPSs are also susceptible to evasion techniques, especially those involving knowledge of a product's channel scanning scheme. Channel scanning can also impact network forensics because each sensor sees only a fraction of the activity on each channel. Wireless IDPS sensors are also susceptible to denial of service attacks and physical attacks. Wireless IDPS sensors can offer intrusion prevention capabilities. Some sensors can instruct endpoints to terminate a session and prevent a new session from being established. Some sensors can instruct a switch on the wired network to block network activity for a particular wireless endpoint; however, this method can only block wired network communications and will not stop an endpoint from continuing to perform malicious actions through wireless protocols. Most IDPS sensors allow administrators to specify the prevention capability configuration for each type of alert. Prevention actions can affect sensor monitoring; for example, if a sensor is transmitting signals to terminate connections, it may not be able to perform channel scanning to monitor other communications until it has completed the prevention action. To mitigate this, some sensors have two radios—one for monitoring and detection, and another for performing prevention actions. When selecting sensors, organizations should consider what prevention actions may need to be performed and how the sensor's detection capabilities could be affected by performing prevention actions

Example: Physical (Facility) Security

(Federal-Communications-Commission-Small-Biz-Cyber-Security-Planning-Guide, 2012)

Physical (Facility) Security

1. Recognize the importance of securing your company facilities

The physical security of a facility depends on a number of security decisions that can be identified through a comprehensive risk-management process. The objective of risk management is to identify an achievable level of protection for your company that corresponds as closely as possible to the level of risk without exceeding the risk.

It is easy to think about physical security of your company's facility as merely an exercise in maintaining control of access points and ensuring there is complete visibility in areas that are determined to be of high-risk – either because of the threat of easy public access or because of the value of information located nearby. However, maintaining security of your company's facility also includes the physical environment of public spaces. For instance:

- Employees whose computers have access to sensitive information should not have their computer monitors oriented toward publicly accessible spaces such as reception areas, check-in desks and waiting rooms. Employees should be trained to not write out logins and passwords on small pieces of paper affixed to computer equipment viewable in public spaces.
- Easy-to-grab equipment that could contain sensitive or personally identifiable information – such as laptops, electronic tablets and cell phones – should be located away from public areas. If you have an environment where employees are working in a waiting room or reception area, train them to not leave these types of devices out on their desks unsecured.
- Consider using cable locks as an easy way to increase security for laptop computers. Most laptops feature a lock port for a cable which can be connected to the user's desk. Be sure to store the key to the cable lock in a secure location away from the desk the computer is locked to.
- In cases that extremely sensitive information is stored on a laptop, consider adding a LoJack software system. The software runs unnoticed and allows law enforcement to locate stolen computers more easily and also allows an administrator to wipe the hard drive remotely if necessary.
- Consider implementing a badge identification system for all employees, and train employees to stop and question anyone in the operational business area without a badge or who appears to be an unescorted visitor.

2. Minimize and safeguard printed materials with sensitive information

Probably the most effective way to minimize the risk of losing control of sensitive information from printed materials is to minimize the amount of printed materials that contain sensitive information. Management procedures should limit how many instances and copies of printed reports memoranda and other material containing personally identifiable information exist.

Safeguard copies of material containing sensitive information by providing employees with locking file cabinets or safes. Make it a standard operating procedure to lock up important information. Train employees to understand that simply leaving the wrong printed material on a desk, in view of the general public, can result in consequences that impact the entire company and your customers.

3. Ensure mail security

Your mail center can introduce a wide range of potential threats to your business. Your center's screening and handling processes must be able to identify threats and hoaxes and eliminate or mitigate the risk they pose to facilities, employees and daily operations. Your company should ensure that mail managers understand the range of screening procedures and evaluate them in terms of your specific operational requirements.

4. Dispose of trash securely

Too often, sensitive information – including customers' personally identifiable information, business financial and other data, and company system access information – is available for anyone to find in the trash. Invest in business grade shredders and buy enough of them to make it convenient for employees. Alternatively, subscribe to a trusted shredding company that will provide locked containers for storage until documents are shredded. Develop standard procedures and employee training programs to ensure that everyone in your company is aware of what types of information need to be shredded.

5. Dispose electronic equipment securely

Be aware that emptying the recycle bin on your desktop or deleting documents from folders on your computer or other electronic device may not delete information forever. Those with advanced computer skills can still access your information even after you think you've destroyed it.

Disposing of electronic equipment requires skilled specialists in order to ensure the security of sensitive information contained within that equipment. If outside help, such as an experienced electronic equipment recycler and data security vendor, is not available or too expensive, you should at a minimum remove computer hard drives and have them shredded. Also, be mindful of risks with other types of equipment associated with computer equipment, including CDs and thumb drives.

6. Train your employees in facility security procedures

A security breach of customer information or a breach of internal company information can result in a public loss of confidence in your company and can be as devastating for your business as a natural disaster. In order to address such risks, you must devote your time, attention and resources (including employee training time) to the potential vulnerabilities in your business environment and the procedures and practices that must be a standard part of each employee's workday.

And while formal training is important to maintaining security, the daily procedures you establish in both the normal conduct of business and in the way you model good security behaviors and practices are equally important. In short, security training should be stressed as critical and reinforced via daily procedures and leadership modeling.

Example Operational (Organizational) Security

(Federal-Communications-Commission-Small-Biz-Cyber-Security-Planning-Guide, 2012)

Operational (Organizational) Security -- OPSEC

While operational security, or OPSEC, has its origins in securing information important to military operations, it has applications across the business community today.
In a commercial context, OPSEC is the process of denying hackers access to any information about the capabilities or intentions of a business by identifying, controlling and protecting evidence of the planning and execution of activities that are essential the success of operations.
OPSEC is a continuous process that consists of five distinct actions:

- Identify information that is critical to your business.
- Analyze the threat to that critical information.

- Analyze the vulnerabilities to your business that would allow a cyber-criminal to access critical information.
- Assess the risk to your business if the vulnerabilities are exploited.
- Apply countermeasures to mitigate the risk factors.

In addition to being a five-step process, OPSEC is also a mindset that all business employees should embrace. By educating oneself on OPSEC risks and methodologies, protecting sensitive information that is critical to the success of your business becomes second nature.

This section explains the OPSEC process and provides some general guidelines that are applicable to most businesses. An understanding of the following terms is required before the process can be explained:

- *Critical information* – Specific data about your business strategies and operations that are needed by cyber criminals to hamper or harm your business from successfully operating.
- *OPSEC indicators* – Business operations and publicly available information that can be interpreted or pieced together by a cyber-criminal to derive critical information.
- *OPSEC vulnerability* – A condition in which business operations provide OPSEC indicators that may be obtained and accurately evaluated by a cyber-criminal to provide a basis for hampering or harming successful business operations.

Cyber Plan Action Items:

1. Identity of critical information

The identification of critical information is important in that it focuses the remainder of the OPSEC process on protecting vital information rather than attempting to protect all information relevant to business operations. Given that any business has limited time, personnel and money for developing secure business practices, it is essential to focus those limited resources on protecting information that is most critical to successful business operations.

Examples of critical information include, but should not be limited to, the following:

- Customer lists and contact information
- Contracts
- Patents and intellectual property
- Leases and deeds
- Policy manuals
- Articles of incorporation
- Corporate papers
- Laboratory notebooks
- Audio tapes
- Video tapes
- Photographs and slides
- Strategic plans and board meeting minutes

Importantly, what is critical information for one business may not be critical for another business. Use your company's mission as a guide for determining what data are truly vital.

2. Analyze threats

This action involves research and analysis to identify likely cyber criminals who may attempt to obtain critical information regarding your company's operations. OPSEC planners in your business should answer the following critical information questions:

- Who might be a cyber-criminal (e.g. competitors, politically motivated hackers, etc.)?
- What are the cyber criminal's goals?
- What actions might the cyber-criminal take?

- What critical information does the cyber-criminal already have on your company’s operations? (i.e., what is already publicly available?)

3. Analyze vulnerabilities

The purpose of this action is to identify the vulnerabilities of your business in protecting critical information. It requires examining each aspect of security that seeks to protect your critical information and then comparing those indicators with the threats identified in the previous step. Common vulnerabilities for small businesses include the following:

- Poorly secured mobile devices that have access to critical information.
- Lack of policy on what information and networked equipment can be taken home from work or taken abroad on travel.
- Storage of critical information on personal email accounts or other non-company networks.
- Lack of policy on what business information can be posted to or accessed by social network sites.

4. Assess risk

This action has two components. First, OPSEC managers must analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures to mitigate each one. Second, specific OPSEC measures must be selected for execution based upon a risk assessment done by your company’s senior leadership. Risk assessment requires comparing the estimated cost associated with implementing each possible OPSEC measure to the potential harmful effects on business operations resulting from the exploitation of a particular vulnerability.

OPSEC measures may entail some cost in time, resources, personnel or interference with normal operations. If the cost to achieve OPSEC protection exceeds the cost of the harm that an intruder could inflict, then the application of the measure is inappropriate. Because the decision not to implement a particular OPSEC measure entails risks, this step requires your company’s leadership approval.

5. Apply appropriate OPSEC measures

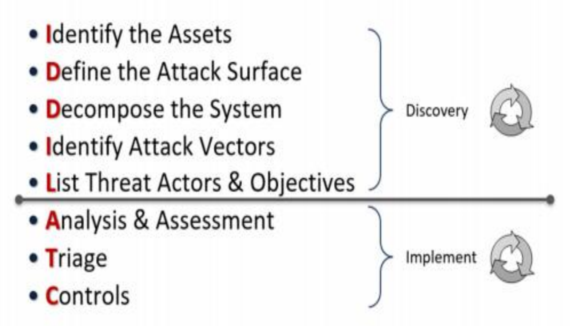
In this action, your company’s leadership reviews and implements the OPSEC measures selected in the assessment of risk action. Before OPSEC measures can be selected, security objectives and critical information must be known, indicators identified and vulnerabilities assessed.

Adversarial Risk

Threat Models – Think like the Attacker

(A-Threat-Driven-Approach-To-Cyber-Security-2019-Muckin&Fitch, 2019)

There Are No Idle Threats – They Attack There is a mnemonic to help remember this methodology: “There are no idle (IDDIL) threats – they attack (ATC)”. There are two phases of work within this methodology: IDDIL is considered the discovery phase and ATC is considered the implementation phase. The phases and their corresponding activities are listed below:

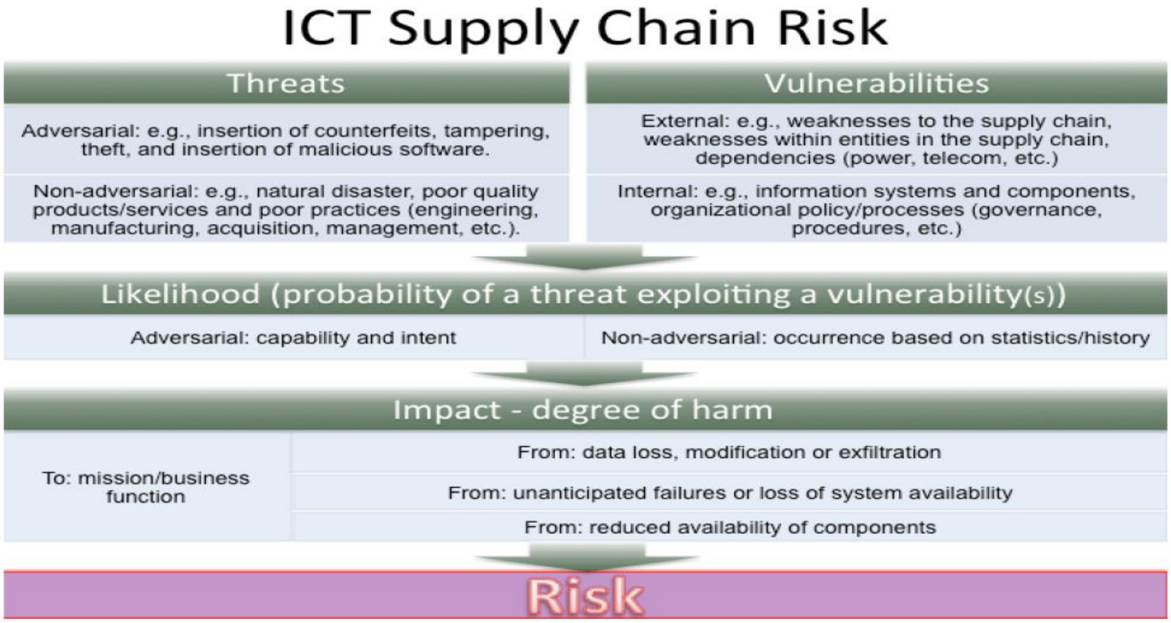


- Business/mission context – Ensure there is an understanding of the business/mission context and impact to business/mission objectives when performing this work.
- Mindset – The team performing the threat analysis must have the skills and capacity to think like an attacker. This trait is critical and directly corresponds to the mindset element presented in the description of the threat-driven approach.
- Iterative – These activities do not need to be sequential. An iterative approach is recommended, and some tasks can be performed in parallel. Completion of all tasks in the methodology is more important than the order in which they are performed. When considered from an enterprise/program/organization perspective versus a discrete project, iterative activities dictate a longer cycle of time and a deeper degree of analysis and integration.
- Brainstorming – To be effective and thorough, the methodology must be a group exercise with proper representation from business, mission and technology stakeholders. Assumptions will be © 2019 Lockheed Martin Corporation 8 necessary and should be documented for follow up. Capture all suggested ideas regarding attacks and weaknesses – they will be prioritized later.
- Time-bounded – Limit the length of time of both individual sessions and overall assessment activities to maximize value versus time spent. This timeframe will vary based on scope and criticality of projects. However, it is necessary to establish time limits for effective project management.

Supply Chain Risk

(NIST-800-161-SupplyChainRiskmanagementpracticesforFederalInformationSystemsandorganizations, 2015)

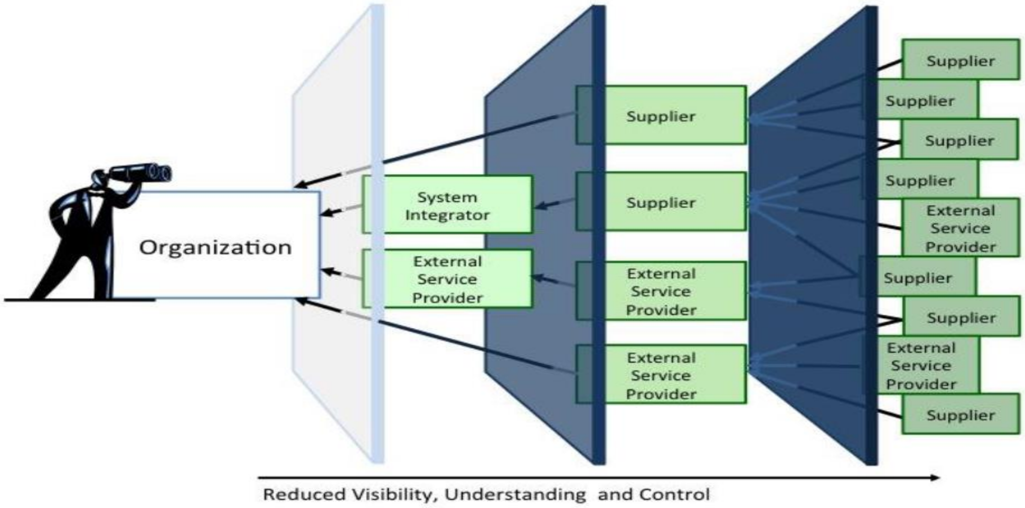
*I*nformation and Communications Technology (ICT) relies on a complex, globally distributed, and interconnected supply chain ecosystem that is long, has geographically diverse routes, and consists of multiple tiers of outsourcing. This ecosystem is composed of public and private sector entities (e.g., acquirers, system integrators, suppliers, and external service providers) and technology, law, policy, procedures, and practices that interact to design, manufacture, distribute, deploy, and use ICT products and services.


ICT Supply Chain Risk
Threats
Adversarial: e.g., insertion of counterfeits, tampering, theft, and insertion of malicious software.
Non-adversarial: e.g., natural disaster, poor quality products/services and poor practices (engineering, manufacturing, acquisition, management, etc.).
Vulnerabilities
External: e.g., weaknesses to the supply chain, weaknesses within entities in the supply chain, dependencies (power, telecom, etc.)
Internal: e.g., information systems and components, organizational policy/processes (governance, procedures, etc.)
Likelihood (probability of a threat exploiting a vulnerability(s))
Adversarial: capability and intent
Non-adversarial: occurrence based on statistics/history
Impact - degree of harm
To: mission/business function
From: data loss, modification or exfiltration
From: unanticipated failures or loss of system availability
From: reduced availability of components
Risk

\

It should be noted that it might take years for a vulnerability stemming from the ICT supply chain to be exploited or discovered. In addition, it may be difficult to determine whether an event was the direct result of a supply chain vulnerability. This may result in a persistent negative impact on an organization's missions that could range from reduction in service levels leading to customer dissatisfaction to theft of intellectual property or degradation of mission-critical functions.

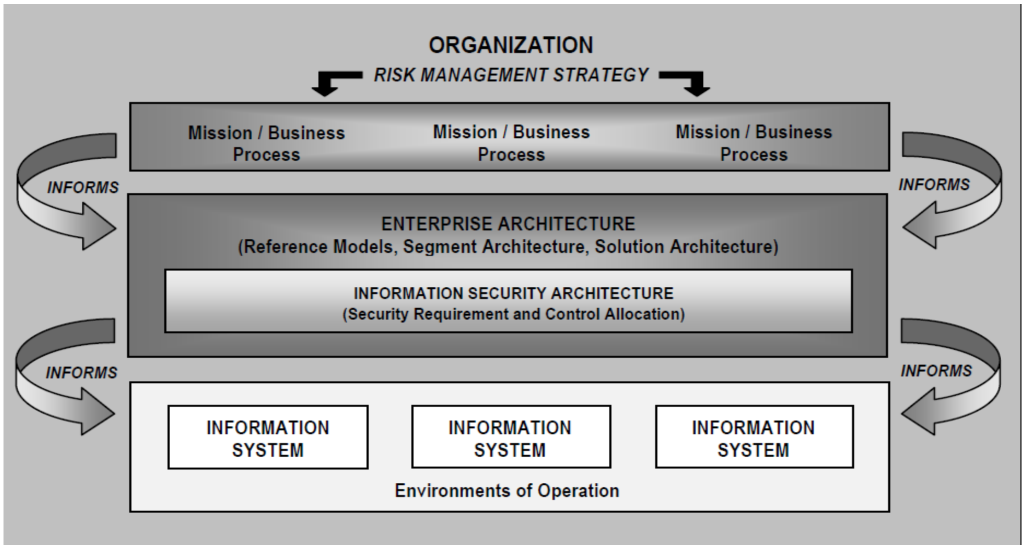
ICT supply chain risks are associated with an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed. They are also associated with the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. Federal agencies have a variety of relationships with their system integrators, suppliers, and external service providers. Figure 1-4 depicts how the diverse types of these relationships affect an organization's visibility and control of the supply chain.


Organization
System Integrator
External Service Provider
Supplier
Supplier
External Service Provider
External Service Provider
Supplier
Supplier
Supplier
Supplier
External Service Provider
Supplier
Supplier
External Service Provider
Supplier
Reduced Visibility, Understanding and Control

Determine Critical Risk

Example (Integrating Risk Management Strategy into Security Requirements – NIST 800-39)

(NIST-Managing-Information-Security-Risk-800-39, 2011)


ORGANIZATION
RISK MANAGEMENT STRATEGY
Mission / Business Process
Mission / Business Process
Mission / Business Process
INFORMS
INFORMS
ENTERPRISE ARCHITECTURE
(Reference Models, Segment Architecture, Solution Architecture)
INFORMATION SECURITY ARCHITECTURE
(Security Requirement and Control Allocation)
INFORMS
INFORMS
INFORMATION SYSTEM
INFORMATION SYSTEM
INFORMATION SYSTEM
Environments of Operation

Risk management considerations can be addressed as an integral part of the enterprise architecture by:

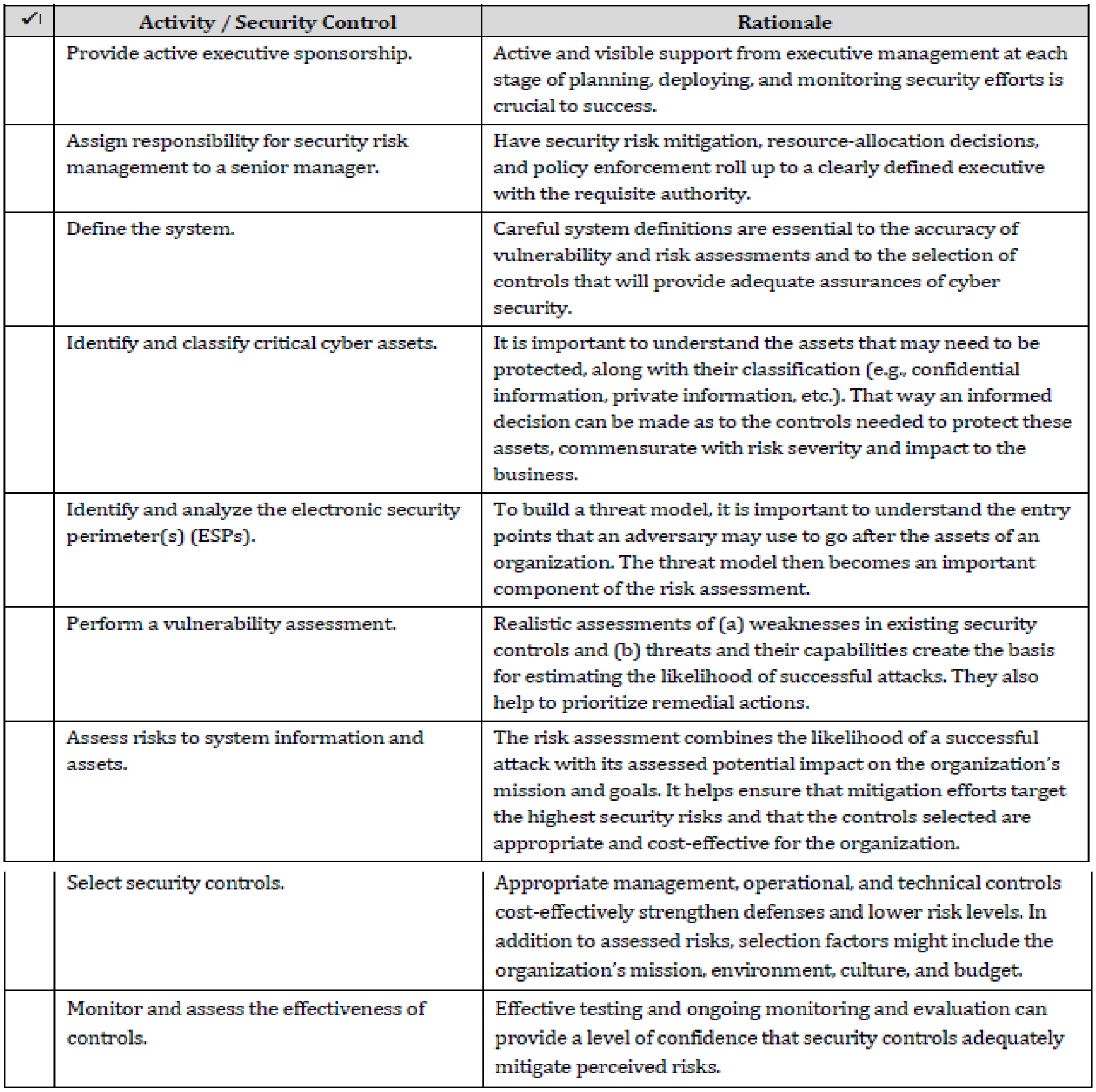
- Developing a segment architecture linked to the strategic goals and objectives of organizations, defined missions/business functions, and associated mission/business processes
- Identifying where effective risk response is a critical element in the success of organizational missions and business functions
- Defining the appropriate, architectural-level information security requirements within organization-defined segments based on the organization’s risk management strategy;
- Incorporating an information security architecture that implements architectural-level information security requirements
- Translating the information security requirements from the segment architecture into specific security controls for information systems/environments of operation as part of the solution architecture
- Allocating management, operational, and technical security controls to information systems and environments of operation as defined by the information security architecture
- Documenting risk management decisions at all levels of the enterprise architecture.

Example (Build a Risk Management Program – NRECA)

(NRECAGuidetoDevelopingaCyberSecurityandRiskMitigationPlan, 2011)

Build Risk Management Program

No usable system is 100 percent secure or impenetrable. The goal of a risk management program is to identify the risks, understand their likelihood and impact on the business, and then put in place security controls that mitigate the risks to a level acceptable to the organization. In addition to assessment and mitigation, a robust risk management program includes ongoing evaluation and assessment of cyber security risks and controls throughout the life cycle of smart grid component software. The following checklist summarizes security best practices and controls that you should consider implementing. This section includes details about the practices.



✓	Activity / Security Control	Rationale
	Provide active executive sponsorship.	Active and visible support from executive management at each stage of planning, deploying, and monitoring security efforts is crucial to success.
	Assign responsibility for security risk management to a senior manager.	Have security risk mitigation, resource-allocation decisions, and policy enforcement roll up to a clearly defined executive with the requisite authority.
	Define the system.	Careful system definitions are essential to the accuracy of vulnerability and risk assessments and to the selection of controls that will provide adequate assurances of cyber security.
	Identify and classify critical cyber assets.	It is important to understand the assets that may need to be protected, along with their classification (e.g., confidential information, private information, etc.). That way an informed decision can be made as to the controls needed to protect these assets, commensurate with risk severity and impact to the business.
	Identify and analyze the electronic security perimeter(s) (ESPs).	To build a threat model, it is important to understand the entry points that an adversary may use to go after the assets of an organization. The threat model then becomes an important component of the risk assessment.
	Perform a vulnerability assessment.	Realistic assessments of (a) weaknesses in existing security controls and (b) threats and their capabilities create the basis for estimating the likelihood of successful attacks. They also help to prioritize remedial actions.
	Assess risks to system information and assets.	The risk assessment combines the likelihood of a successful attack with its assessed potential impact on the organization's mission and goals. It helps ensure that mitigation efforts target the highest security risks and that the controls selected are appropriate and cost-effective for the organization.
	Select security controls.	Appropriate management, operational, and technical controls cost-effectively strengthen defenses and lower risk levels. In addition to assessed risks, selection factors might include the organization's mission, environment, culture, and budget.
	Monitor and assess the effectiveness of controls.	Effective testing and ongoing monitoring and evaluation can provide a level of confidence that security controls adequately mitigate perceived risks.

Example (Build Risk Management Approach - University of South Florida IT Security Plan)

Risk Management Approaches

USF IT will manage risk by identifying, evaluating, controlling, and mitigating vulnerabilities that are a potential threat to the data and information systems under its control; it will execute its defined risk management process on an ongoing basis, periodically assessing risks and implementing new controls in response to changes in its information systems as well as to changes to federal, state, and USF regulations and policies.

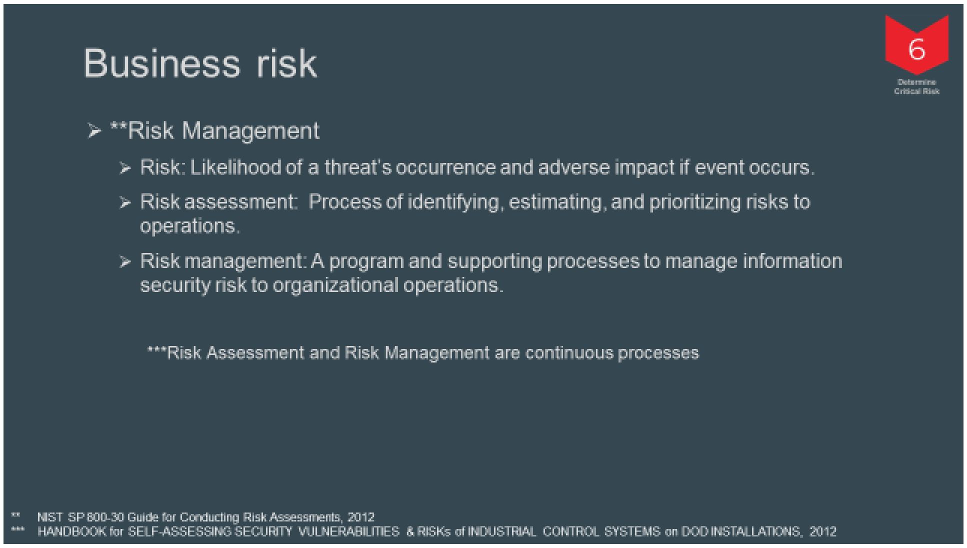
- Risk assessments will be performed on all new systems or on systems undergoing significant change before they are moved into active production stage, and appropriate measures will be taken to address the risks associated with identified vulnerabilities.
- Annual risk assessments will be performed on active production information systems, and appropriate measures will be taken to address the risk associated with identified vulnerabilities.
- Vulnerability or threat notifications from vendors and other appropriate sources will be monitored and assessed for all systems and applications associated with any USF information system.
- When required, security authorization for USF information systems to operate with security risks that have been evaluated and determined to be acceptable will be obtained from the OIS Director.

Example (Identify Critical Risk – Dept. of Homeland Security Evaluation/Analysis 401)

(NIST-GuideforConductingRiskAssessments-800-30-R1, 2012)

(NIST-Managing-Information-Security-Risk-800-39, 2011)

BASIC Risk Management Approach



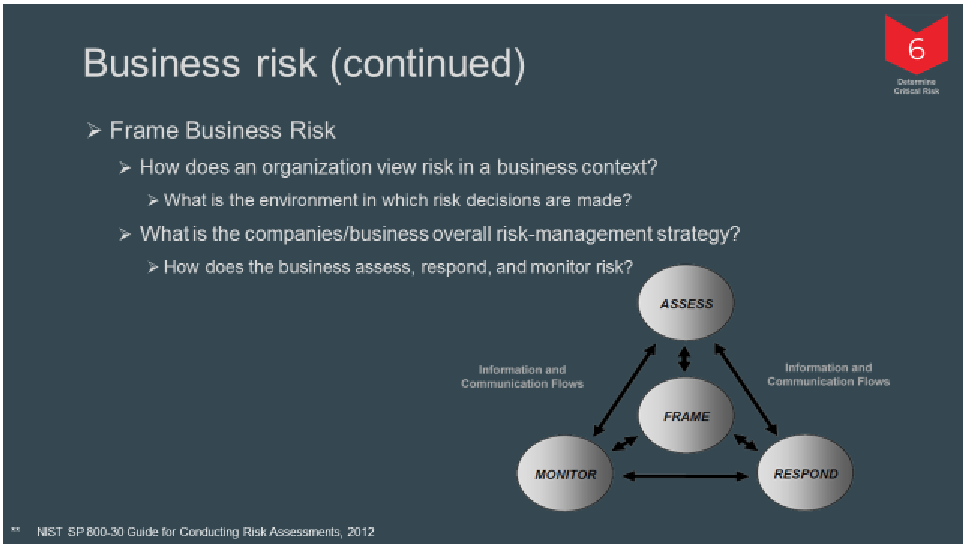
Business risk

6
Determine Critical Risk

- **Risk Management
  - Risk: Likelihood of a threat's occurrence and adverse impact if event occurs.
  - Risk assessment: Process of identifying, estimating, and prioritizing risks to operations.
  - Risk management: A program and supporting processes to manage information security risk to organizational operations.

***Risk Assessment and Risk Management are continuous processes

** NIST SP 800-30 Guide for Conducting Risk Assessments, 2012
*** HANDBOOK for SELF-ASSESSING SECURITY VULNERABILITIES & RISKs of INDUSTRIAL CONTROL SYSTEMS on DOD INSTALLATIONS, 2012



Business risk (continued)

- Frame Business Risk
  - How does an organization view risk in a business context?
    - What is the environment in which risk decisions are made?
  - What is the companies/business overall risk-management strategy?
    - How does the business assess, respond, and monitor risk?

ASSESS

Information and Communication Flows

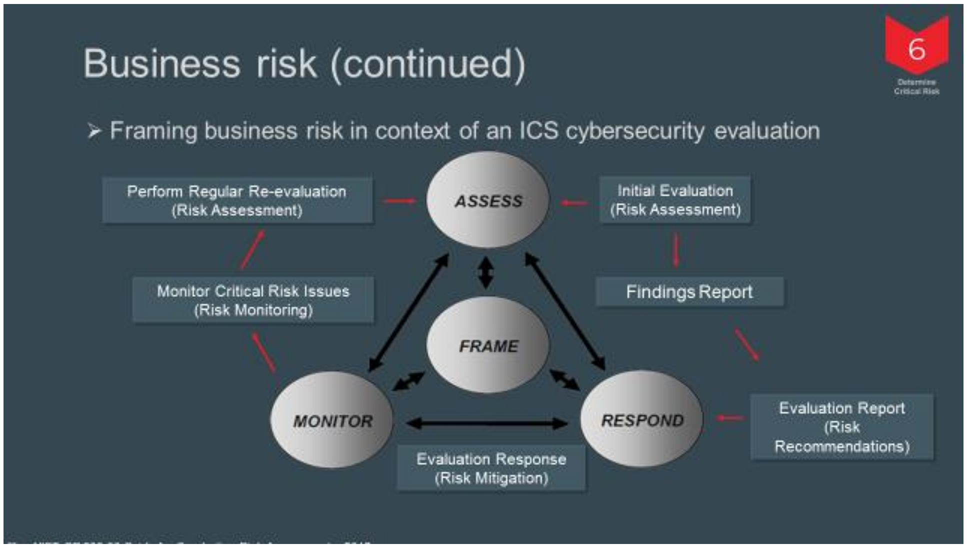
Information and Communication Flows

FRAME

MONITOR

RESPOND

** NIST SP 800-30 Guide for Conducting Risk Assessments, 2012



Business risk (continued)

- Framing business risk in context of an ICS cybersecurity evaluation

Perform Regular Re-evaluation (Risk Assessment)

ASSESS

Initial Evaluation (Risk Assessment)

Monitor Critical Risk Issues (Risk Monitoring)

Findings Report

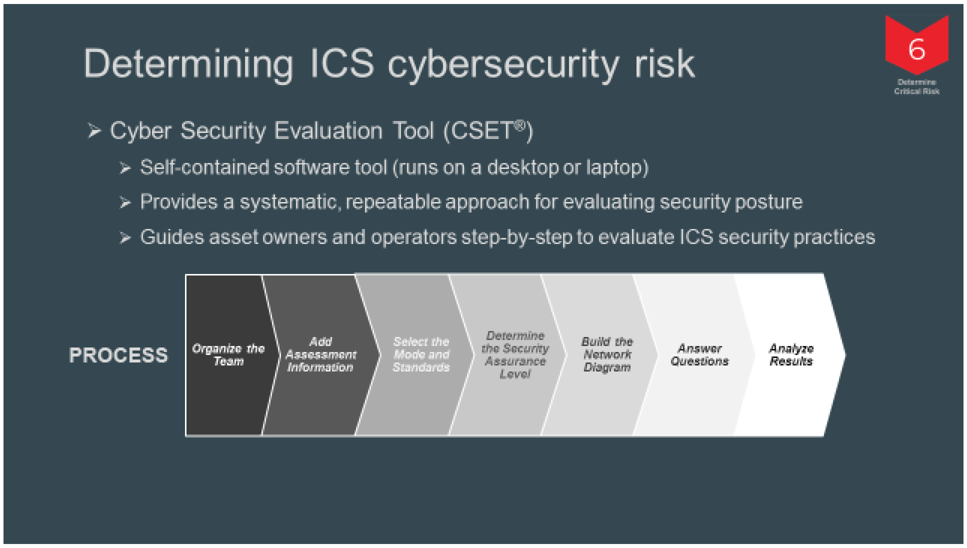
FRAME

MONITOR

RESPOND

Evaluation Report (Risk Recommendations)

Evaluation Response (Risk Mitigation)



Determining ICS cybersecurity risk

- Cyber Security Evaluation Tool (CSET®)
  - Self-contained software tool (runs on a desktop or laptop)
  - Provides a systematic, repeatable approach for evaluating security posture
  - Guides asset owners and operators step-by-step to evaluate ICS security practices

PROCESS

Organize the Team

Add Assessment Information

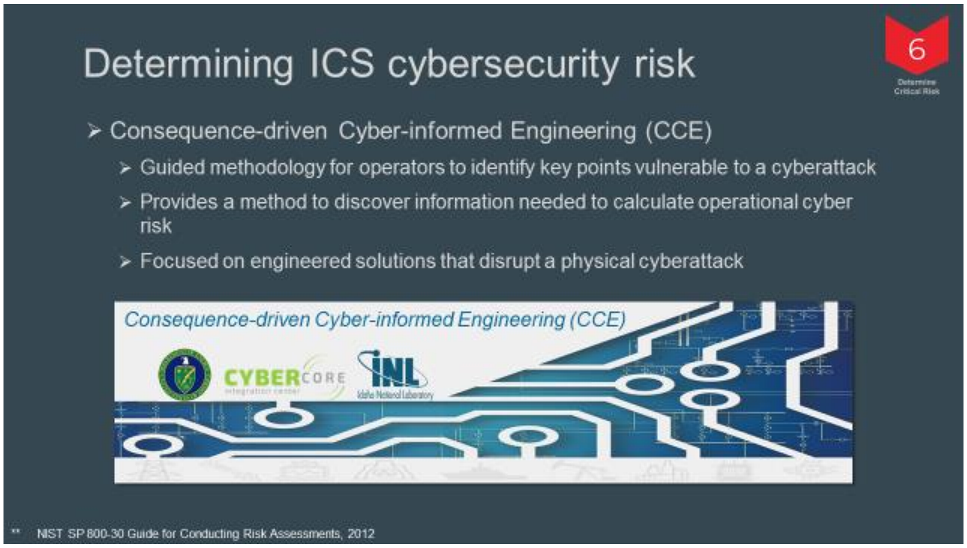
Select the Mode and Standards

Determine the Security Assurance Level

Build the Network Diagram

Answer Questions

Analyze Results



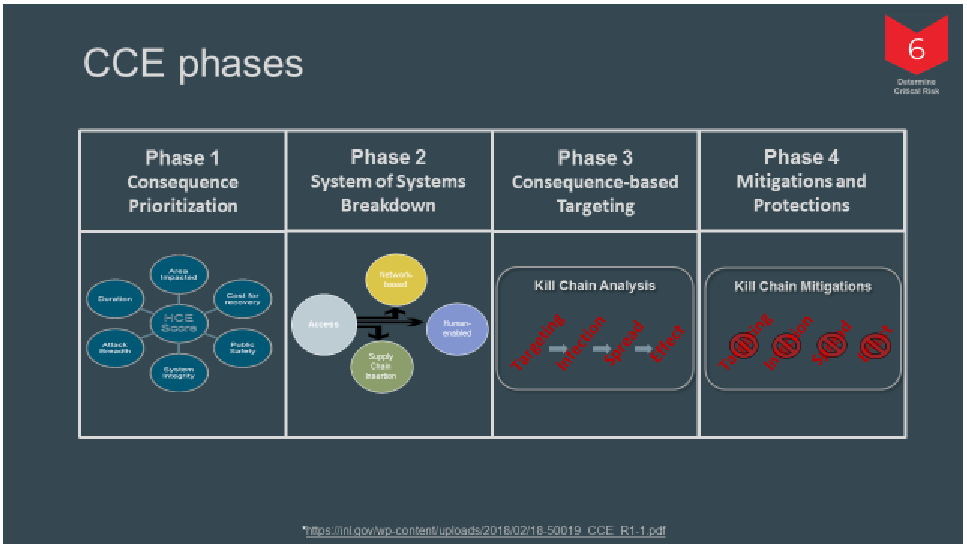
Determining ICS cybersecurity risk

6
Determine Critical Risk

- Consequence-driven Cyber-informed Engineering (CCE)
  - Guided methodology for operators to identify key points vulnerable to a cyberattack
  - Provides a method to discover information needed to calculate operational cyber risk
  - Focused on engineered solutions that disrupt a physical cyberattack

Consequence-driven Cyber-informed Engineering (CCE)
CYBERCORE
integration center
INL
Idaho National Laboratory

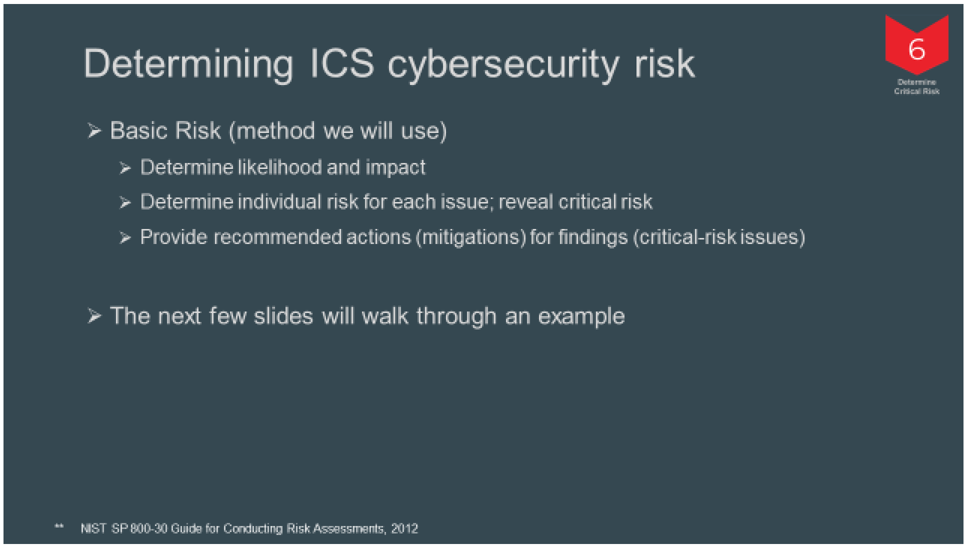
** NIST SP 800-30 Guide for Conducting Risk Assessments, 2012



CCE phases

Phase 1 Consequence Prioritization	Phase 2 System of Systems Breakdown	Phase 3 Consequence-based Targeting	Phase 4 Mitigations and Protections
		Kill Chain Analysis	Kill Chain Mitigations

*https://inl.gov/wp-content/uploads/2018/02/18-50019_CCE_R1-1.pdf



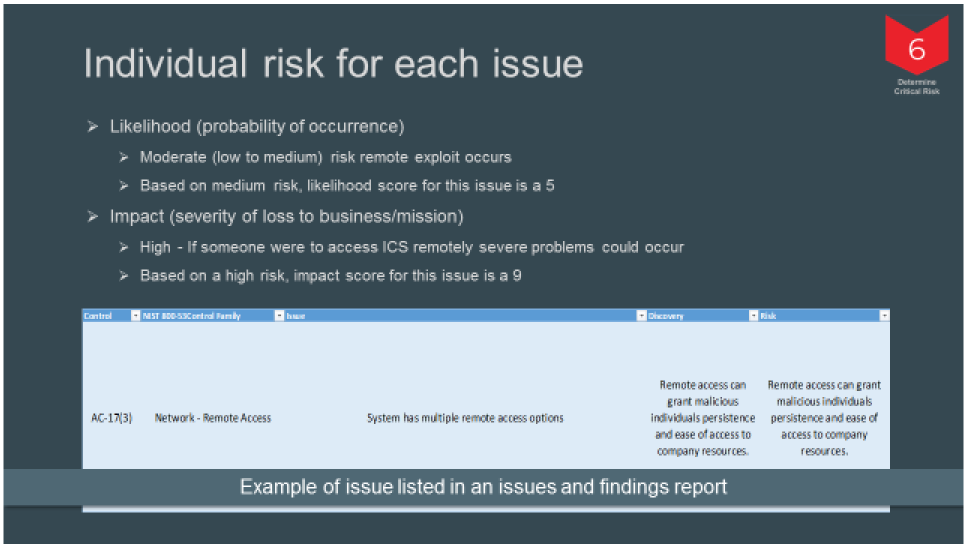
Determining ICS cybersecurity risk

6
Determine Critical Risk

- Basic Risk (method we will use)
  - Determine likelihood and impact
  - Determine individual risk for each issue; reveal critical risk
  - Provide recommended actions (mitigations) for findings (critical-risk issues)

- The next few slides will walk through an example

** NIST SP 800-30 Guide for Conducting Risk Assessments, 2012



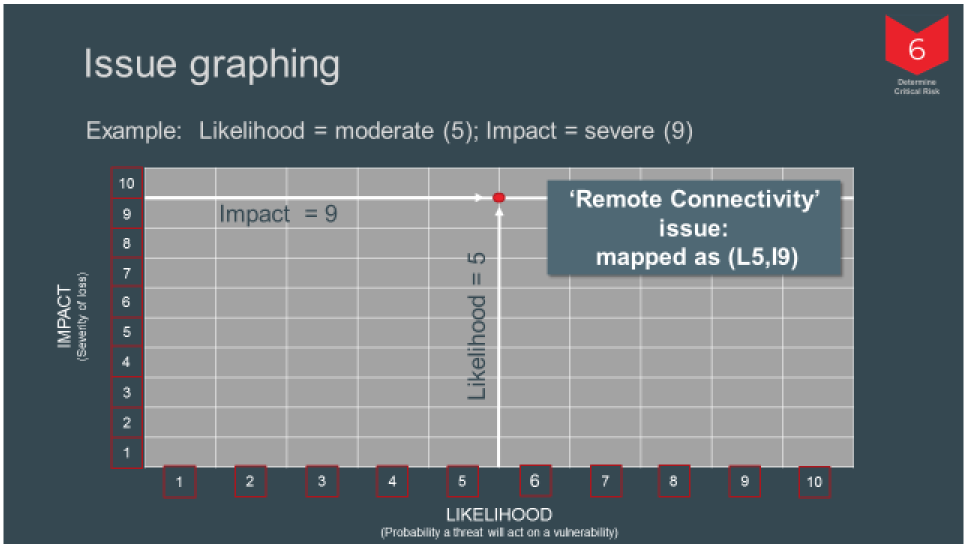
Individual risk for each issue

6 Determine Critical Risk

- Likelihood (probability of occurrence)
  - Moderate (low to medium) risk remote exploit occurs
  - Based on medium risk, likelihood score for this issue is a 5
- Impact (severity of loss to business/mission)
  - High - If someone were to access ICS remotely severe problems could occur
  - Based on a high risk, impact score for this issue is a 9

Control	NIST 800-53Control Family	Issue	Discovery	Risk
AC-17(3)	Network - Remote Access	System has multiple remote access options	Remote access can grant malicious individuals persistence and ease of access to company resources.	Remote access can grant malicious individuals persistence and ease of access to company resources.

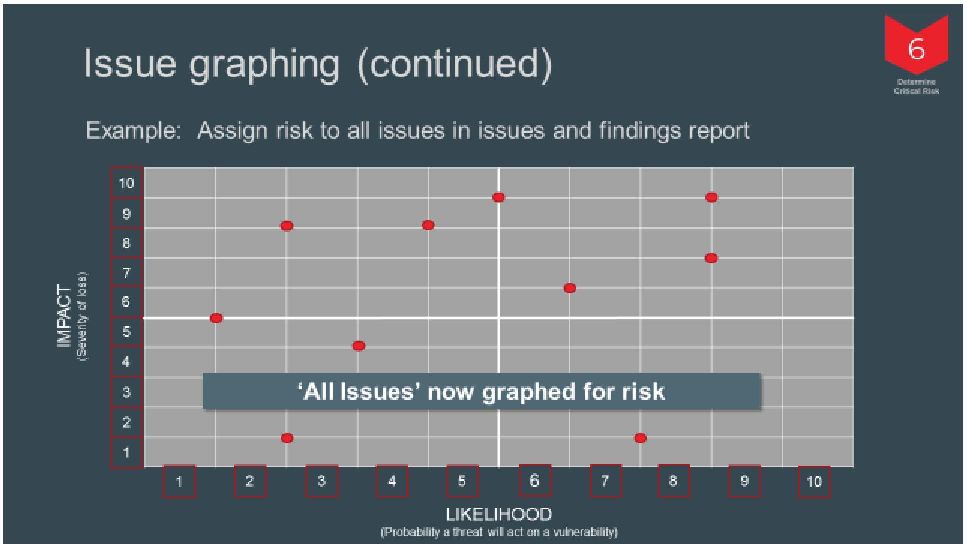
Example of issue listed in an issues and findings report



Issue graphing

6 Determine Critical Risk

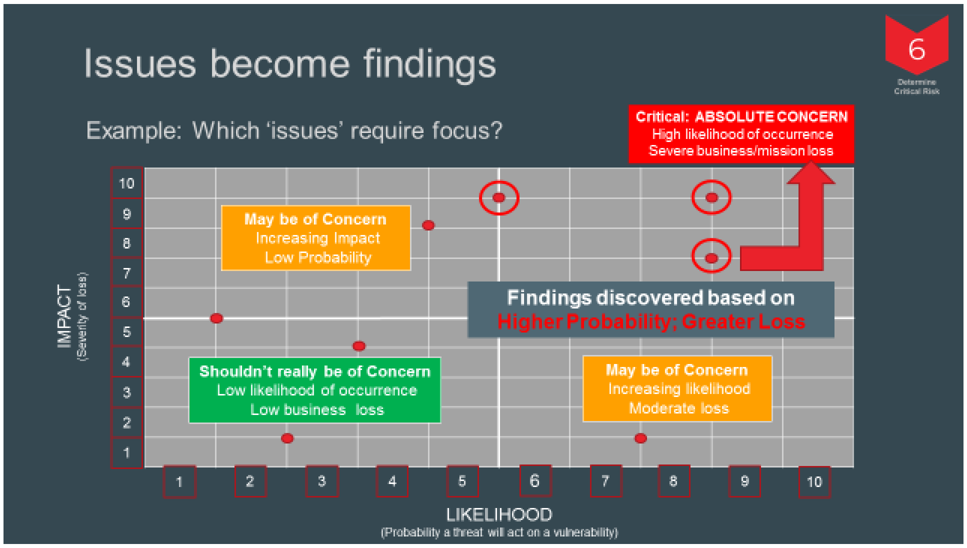
Example: Likelihood = moderate (5); Impact = severe (9)



Issue graphing (continued)

6 Determine Critical Risk

Example: Assign risk to all issues in issues and findings report



Issues become findings

Example: Which 'issues' require focus?

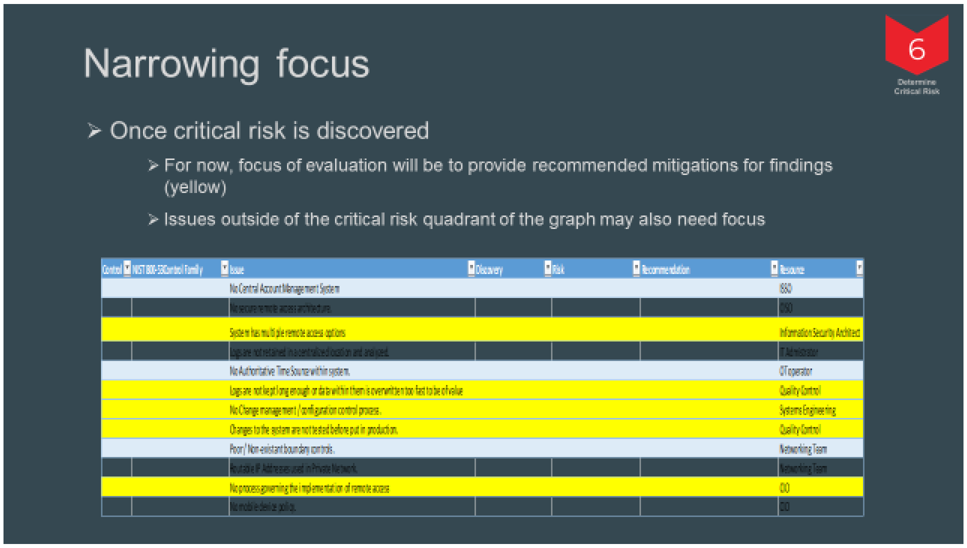
Critical: ABSOLUTE CONCERN
High likelihood of occurrence
Severe business/mission loss

May be of Concern
Increasing Impact
Low Probability

Findings discovered based on
Higher Probability; Greater Loss

Shouldn't really be of Concern
Low likelihood of occurrence
Low business loss

May be of Concern
Increasing likelihood
Moderate loss



Narrowing focus

- Once critical risk is discovered
  - For now, focus of evaluation will be to provide recommended mitigations for findings (yellow)
  - Issues outside of the critical risk quadrant of the graph may also need focus

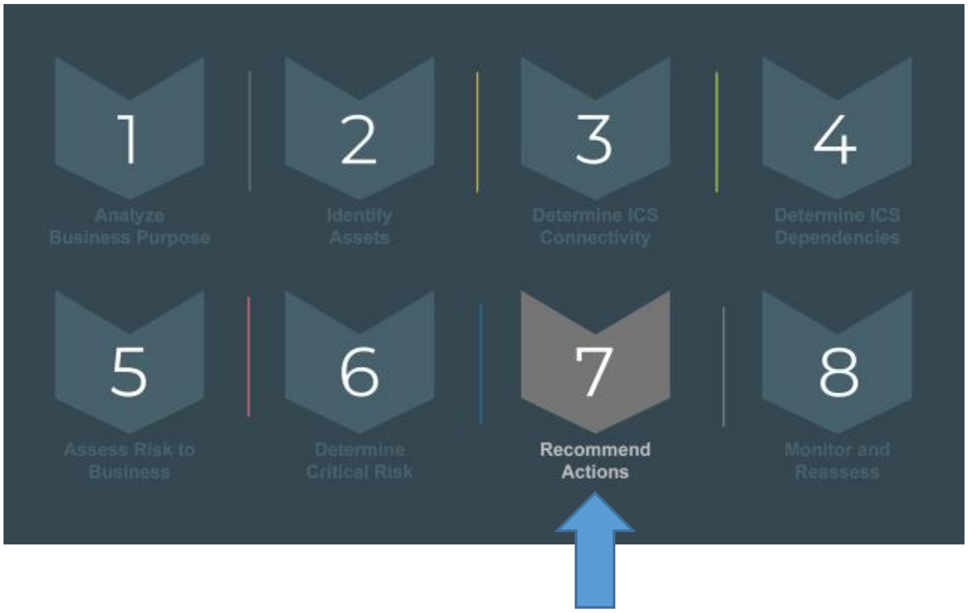
Control	NIST 800-53Control Family	Issue	Discovery	Risk	Recommendation	Resource
		No Central Account Management System				ISSO
		No secure remote access architecture.				CISO
		System has multiple remote access options				Information Security Architect
		Logs are not retained in a centralized location and analyzed.				IT Administrator
		No Authoritative Time Source within system.				OT operator
		Logs are not kept long enough or data within them is overwritten too fast to be of value				Quality Control
		No Change management / configuration control process.				Systems Engineering
		Changes to the system are not tested before put in production.				Quality Control
		Poor / Non-existant boundary controls.				Networking Team
		Routable IP Addresses used in Private Network.				Networking Team
		No process governing the implementation of remote access				CIO
		No mobile device policy.				CIO

Recommend Actions

Establish Evaluation (Assessment) Expected Outcomes and Products

Example: Evaluation (Assessment Process) – with step to Recommend Actions

(Handbook-for-Self-Assessing_Security_Vulnerabilities&Risks_of_Industrial_Control_Systems_on_DOD_Installations, 2012)



1 Analyze Business Purpose

2 Identify Assets

3 Determine ICS Connectivity

4 Determine ICS Dependencies

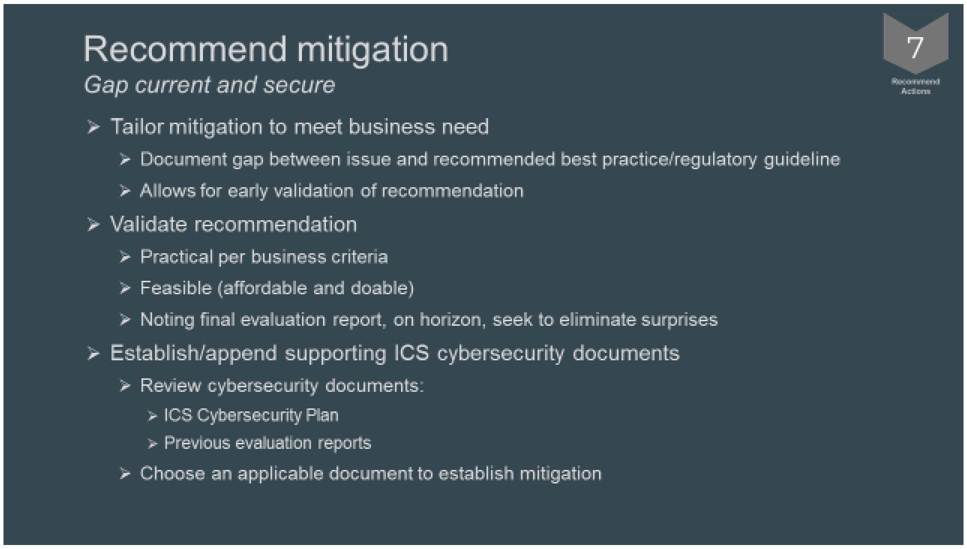
5 Assess Risk to Business

6 Determine Critical Risk

7 Recommend Actions

8 Monitor and Reassess

Establish outcomes for each issue discovered during assessment

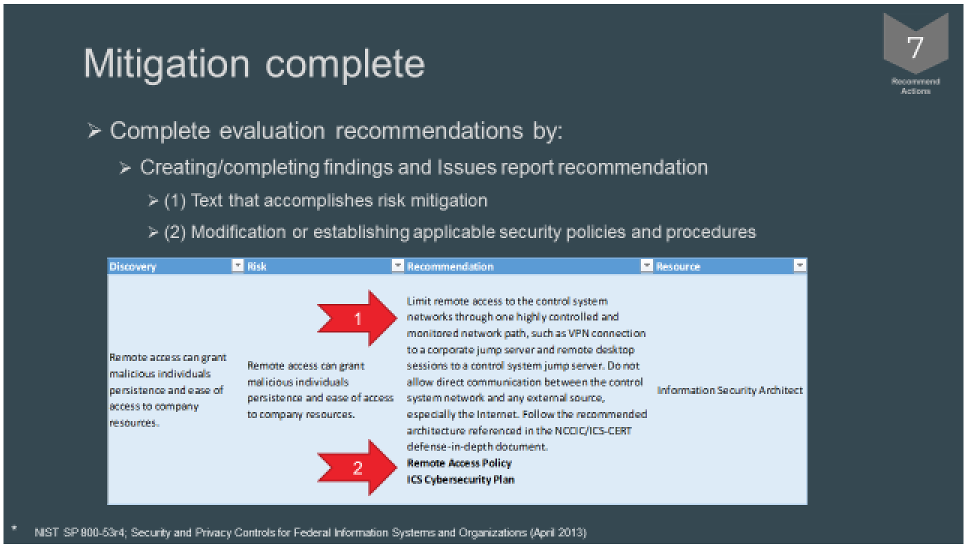


7
Recommend Actions

Recommend mitigation

Gap current and secure

- Tailor mitigation to meet business need
  - Document gap between issue and recommended best practice/regulatory guideline
  - Allows for early validation of recommendation
- Validate recommendation
  - Practical per business criteria
  - Feasible (affordable and doable)
  - Noting final evaluation report, on horizon, seek to eliminate surprises
- Establish/append supporting ICS cybersecurity documents
  - Review cybersecurity documents:
    - ICS Cybersecurity Plan
    - Previous evaluation reports
  - Choose an applicable document to establish mitigation


7
Recommend Actions
1
2

Mitigation complete

- Complete evaluation recommendations by:
  - Creating/completing findings and Issues report recommendation
    - (1) Text that accomplishes risk mitigation
    - (2) Modification or establishing applicable security policies and procedures

Discovery	Risk	Recommendation	Resource
Remote access can grant malicious individuals persistence and ease of access to company resources.	Remote access can grant malicious individuals persistence and ease of access to company resources.	Limit remote access to the control system networks through one highly controlled and monitored network path, such as VPN connection to a corporate jump server and remote desktop sessions to a control system jump server. Do not allow direct communication between the control system network and any external source, especially the Internet. Follow the recommended architecture referenced in the NCCIC/ICS-CERT defense-in-depth document. **Remote Access Policy** **ICS Cybersecurity Plan**	Information Security Architect

* NIST SP 800-53r4; Security and Privacy Controls for Federal Information Systems and Organizations (April 2013)

Verify that your finding 'text' is supported by a regulatory standard or best practice. For example, one can use a number of documents to provide evidence for recommendations such as NIST 800-53 or CNSSI 1253 and/or many others.

Implement cyber security defense-in-depth architecture

Example Demilitarized Zone (DMZ)

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

Unlike traditional IT systems, ICS/OT systems need to have minimal connectivity to the INL enterprise and are currently self-managed by the owning organization with direct connections to the enterprise network and the Internet. This design has resulted in an absence of enterprise solutions within the ICS environment and an overall failure to consistently apply software quality assurance, configuration management, and cybersecurity best practices. The ICS DMZ will provide a secure environment from which these services can be hosted and provide a barrier between these systems and the enterprise network, while the network segmentation will provide barriers between each of the systems themselves.

The following key capabilities are needed, to enable an effective DMZ and Network Segmentation Plan:

- Provide services within the DMZ so ICS systems do not connect to the enterprise or Internet directly
- Have network segmentation to protection systems from cross contamination
- Effectively and accurate identify vulnerabilities and that exist within INL ICS systems
- Monitor and protect identified systems.
- Create a standard for all system owners and network infrastructure to follow

Example - ICS Cybersecurity Test Lab

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

In support of testing new configurations and security controls, this plan includes the creation of an isolated ICS/OT Cybersecurity Test Lab where proof of concepts, vendor burn-ins, and other pre-production ICS testing can occur

Example -Security Controls selection and documentation

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

The initial set of controls for INL ICS will be selected and implemented according to NIST SP 800-82 and SP 800-53. All INL ICS systems must follow the guidance of these reference standards. The administrative and technical controls must be tailored to meet mission, safety, cost efficiency, operations, and security requirements specific to each system.

Monitor and assess the effectiveness of controls and continuously reassess

Incident Response

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

Cybersecurity incident responses will be conducted in a team approach. Members of the team will vary depending on the incident type, severity, and distribution of the incident. As a minimum, the incident response team will include the owning organization and Cyber Security. Other organizations will be included as additional expertise and resources are needed. Incident response teams must place emphasis on:

- Health and Safety
- Mission support
- Containment of incident to mitigate spreading
- Prevention of data exfiltration
- Communicating to management.
- Unclassified incidents will be conducted in accordance with 'Unclassified', "Cyber Security Incident Response Plan."
- Classified incidents will be conducted in accordance with 'Classified', "Classified Information Spillage."

Technical Continuous Monitoring

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

Many of the technical security controls defined in NIST SP 800-53 are good candidates for monitoring using automated tools and techniques. Real-time monitoring of implemented technical controls using automated tools can provide INL with a much more dynamic view of the effectiveness of those controls and the security posture of the organization. It is important to recognize that with any comprehensive information security program, all implemented security controls, including management and operational controls, must be regularly assessed for effectiveness, even if the monitoring of such controls cannot be automated or is not easily automated.

INL's continuous monitoring program applies a combination of assessment processes and automation tools to provide a comprehensive and broad scope cybersecurity risk management program

Establish Cyber Security Program policies/standards/procedures

Mobile Devices / Communications

(Federal-Communications-Commission-Small-Biz-Cyber-Security-Planning-Guide, 2012)

If your company uses mobile devices to conduct company business, such as accessing company email or sensitive data, pay close attention to mobile security and the potential threats that can expose and compromise your overall business networks. This section describes the mobile threat environment and the practices that small businesses can use to help secure devices such as smartphones, tablets and Wi-Fi enabled laptops.

Many organizations are finding that employees are most productive when using mobile devices, and the benefits are too great to ignore. But while mobility can increase workplace productivity, allowing employees to bring their own mobile devices into the enterprise can create significant security and management challenges.

Data loss and data breaches caused by lost or stolen phones create big challenges, as mobile devices are now used to store confidential business information and access the corporate network. According to a December 2010 Symantec mobile security survey, 68 percent of respondents ranked loss or theft as their top mobile-device security concern, while 56 percent said mobile malware is their number two concern. It is important to remember that while the individual employee may be liable for a device, the company is still liable for the data.

Top threats targeting mobile devices

- *Data Loss* – An employee or hacker accesses sensitive information from device or network. This can be unintentional or malicious, and is considered the biggest threat to mobile devices
- *Social Engineering Attacks* – A cybercriminal attempts to trick users to disclose sensitive information or install malware. Methods include phishing and targeted attacks.
- *Malware* – Malicious software that includes traditional computer viruses, computer worms and Trojan horse programs. Specific examples include the Ikee worm, targeting iOS-based devices; and Pjapps malware that can enroll infected Android devices in a collection of hacker-controlled "zombie" devices known as a "botnet."
- *Data Integrity Threats* – Attempts to corrupt or modify data in order to disrupt operations of a business for financial gain. These can also occur unintentionally.
- *Resource Abuse* – Attempts to misuse network, device or identity resources. Examples include sending spam from compromised devices or denial of service attacks using computing resources of compromised devices.
- *Web and Network-based Attacks* – Launched by malicious websites or compromised legitimate sites, these target a device's browser and attempt to install malware or steal confidential data that flows through it.

Cyber Plan Action Items:

A few simple steps can to help ensure company information is protected. These include requiring all mobile devices that connect to the business network be equipped with security software and password protection; and providing general security training to make employees aware of the importance of security practices for mobile devices. More specific practices are detailed below.

Use security software on all smartphones

Security software specifically designed for smartphones can stop hackers and prevent cyber criminals from stealing your information or spying on you when you use public networks. It can detect and remove viruses and other mobile threats before they cause you problems. It can also eliminate annoying text and multimedia spam messages.

Make sure all software is up to date

Mobile devices must be treated like personal computers in that all software on the devices should be kept current, especially the security software. This will protect devices from new variants of malware and viruses that threaten your company's critical information.

Encrypt the data on mobile devices

Business and personal information stored on mobile devices is often sensitive. Encrypting this data is another must.

If a device is lost and the SIM card stolen, the thief will not be able to access the data if the proper encryption technology is loaded on the device.

Have user's password protect access to mobile devices

In addition to encryption and security updates, it is important to use strong passwords to protect data stored on mobile devices. This will go a long way toward keeping a thief from accessing sensitive data if the device is lost or hacked.

Urge users to be aware of their surroundings

Whether entering passwords or viewing sensitive or confidential data, users should be cautious of who might be looking over their shoulder.

Employ these strategies for email, texting and social networking

Avoid opening unexpected text messages from unknown senders – As with email, attackers can use text messages to spread malware, phishing scams and other threats among mobile device users. The same caution should be applied to opening unsolicited text messages that users have become accustomed to with email.

Don't be lured in by spammers and phishers – To shield business networks from cyber criminals, small businesses should deploy appropriate email security solutions, including spam prevention, which protect a company's reputation and manage risks.

Click with caution – Just like on stationary PCs, social networking on mobile devices and laptops should be conducted with care and caution. Users should not open unidentified links, chat with unknown people or visit unfamiliar sites. It doesn't take much for a user to be tricked into compromising a device and the information on it.

Set reporting procedures for lost or stolen equipment

In the case of a loss or theft, employees and management should all know what to do next. Processes to deactivate the device and protect its information from intrusion should be in place. Products are also available for the automation of such processes, allowing small businesses to breathe easier after such incidents.

Ensure all devices are wiped clean prior to disposal

Most mobile devices have a reset function that allows all data to be wiped. SIM cards should also be removed and destroyed.

Helpful links:

- Teach your employees about mobile apps: http://onguardonline.gov/articles/0018-understanding-mobile-apps
- Keep your laptops secure: http://onguardonline.gov/articles/0015-laptop-security

System /network administration activities

Configuration management; Change management and control

Access Management; security assessment and authorization

Intrusion Detection and Incident Response

(NIST-800-94-GuidetoIntrusionDetectionandPreventionSystems, 2007)

The typical components in an IDPS solution are sensors or agents, management servers, database servers, and consoles. Sensors and agents monitor and analyze activity; sensors are used to monitor networks and agents to monitor hosts. Management servers receive information from sensors or agents and manage them. Database servers are repositories for event information recorded by the sensors or agents and management servers. Consoles are programs that provide interfaces for IDPS users and administrators. These components can be connected to each other through an organization’s standard networks or through a separate network strictly designed for security software management known as a management network. A management network helps to protect the IDPS from attack and to ensure it has adequate bandwidth under adverse conditions. A virtual management network can be created using a virtual local area network (VLAN); this provides protection for IDPS communications, but not as much protection as a management network would provide. Most IDPSs can provide a wide variety of security capabilities. Some products offer information gathering capabilities, such as collecting information on hosts or networks from observed activity. IDPSs also typically perform extensive logging of data related to detected events. This data can be used to confirm the validity of alerts, investigate incidents, and correlate events between the IDPS and other logging sources. Generally, logs should be stored both locally and centrally to support the integrity and availability of the data. IDPSs typically offer extensive, broad detection capabilities. The types of events detected and the typical accuracy of detection vary greatly depending on the type of IDPS technology. Most IDPSs require at least some tuning and customization to improve their detection accuracy, usability, and effectiveness. Typically, the more powerful a product’s tuning and customization capabilities are, the more its detection accuracy can be improved from the default configuration. Examples of these capabilities are thresholds, blacklists and whitelists, alert settings, and code editing. Organizations should carefully consider the tuning and customization capabilities of IDPSs when evaluating products. Administrators should review tuning and customizations periodically to ensure that they are still accurate. Administrators should also ensure that any products collecting baselines for anomaly-based detection have those baselines rebuilt periodically as needed to support accurate detection. Most IDPSs offer multiple prevention capabilities; the specific capabilities vary by IDPS technology type. IDPSs usually allow administrators to specify the prevention capability configuration for each type of alert. This includes enabling or disabling prevention, as well as specifying which type of prevention capability should be used. Once an IDPS product has been selected, the administrators need to design an architecture, perform IDPS component testing, and deploy and secure the IDPS components. There are many architectural considerations, including component placement, solution reliability, interoperability with other systems, management network architecture, and necessary changes to other security controls. Before performing a production implementation, organizations should consider implementing the components in a test environment first to reduce the likelihood of implementation problems disrupting production. When the components are being deployed to production networks, organizations should initially activate only a few IDPS sensors or agents. Because a new deployment is likely to generate a large number of false positives until fully tuned and customized, activating many sensors or agents at once might overwhelm the management servers and consoles, making it difficult for administrators to perform tuning and customization.

Incident Response and Reporting

Security Audits

Exemptions / Exceptions

Staff SDLC Security Task Orientation

Security Profile Objectives

System profile

System Architecture / decomposition

Test Data Creation

Accreditation (Executive Level Sign-off)

System Disposal

Physical and Personnel Security

System and Information Integrity

Planning

Audit & Accountability Control Requirements

Identification & Authorization Control Requirements

System & Communications Control Requirements

Virtualization Technologies

Cloud Computing Technologies

Example - Cloud Services

(INL-UnclassifiedCyberSecurityProcedure, 2019)

Cloud computing services include any external information system(s) that provide services, software, or infrastructure (servers, storage, processing, or networking) delivered or used on-demand over the Internet.

ISSM: Reviews and approves all enterprise cloud service risk assessments prior to submission.

Cyber Security: Assess the risk of current or planned use of cloud services.

Identify and monitor the usage of authorized and unauthorized cloud services.

Assist ISSOs or service owners in identifying security responsibilities when managing and using cloud services.

Provide minimum cybersecurity requirements for cloud services used:

Service risk levels are determined based on the Risk score as follows.

1–3 = low risk

4–6 = moderate risk

7+ = high risk (The service cannot be approved unless overridden by ISSM.)

Security awareness and training

Security concerns in system management

Additional System and Communication Protections

Service Continuity Management

Situational awareness

Scams and Fraud

Network Security

Web site security

E-mail

(Federal-Communications-Commission-Small-Biz-Cyber-Security-Planning-Guide, 2012)

Email has become a critical part of our everyday business, from internal management to direct customer support.

The benefits associated with email as a primary business tool far outweigh the negatives. However, businesses must be mindful that a successful email platform starts with basic principles of email security to ensure the privacy and protection of customer and business information.

Cyber Plan Action Items:

Set up a spam email filter

It has been well documented that spam, phishing attempts and otherwise unsolicited and unwelcome email often accounts for more than 60 percent of all email that an individual or business receives. Email is the primary method for spreading viruses and malware and it is one of the easiest to defend against. Consider using email-filtering services that your email service, hosting provider or other cloud providers offer. A local email filter application is also an important component of a solid antivirus strategy. Ensure that automatic updates are enabled on your email application, email filter and anti-virus programs. Ensure that filters are reviewed regularly so that important email and/or domains are not blocked in error.

Train your employees in responsible email usage

The last line of defense for all of your cyber risk efforts lies with the employees who use tools such as email and their responsible and appropriate use and management of the information under their control. Technology alone cannot make a business secure. Employees must be trained to identify risks associated with email use, how and when to use email appropriate to their work, and when to seek assistance of professionals. Employee awareness training is available in many forms, including printed media, videos and online training.

Consider requiring security awareness training for all new employees and refresher courses every year. Simple efforts such as monthly newsletters, urgent bulletins when new viruses are detected, and even posters in common areas to remind your employees of key security and privacy to-do’s create a work environment that is educated in protecting your business.

Protect sensitive information sent via email

With its proliferation as a primary tool to communicate internally and externally, business email often includes sensitive information. Whether it is company information that could harm your business or regulated data such as personal health information (PHI) or personally identifiable information (PII), it is important to ensure that such information is only sent and accessed by those who are entitled to see it. Since email in its native form is not designed to be secure, incidents of misaddressing or other common accidental forwarding can lead to data leakage. Businesses that handle this type of information should consider whether such information should be sent via email, or at least consider using email encryption. Encryption is the process of converting data into unreadable format to prevent disclosure to unauthorized personnel. Only individuals or organizations with access to the encryption key can read the information. Other cloud services offer “Secure Web

Enabled Drop Boxes” that enable secure data transfer for sensitive information, which is often a better approach to transmitting between companies or customers.

Set a sensible email retention policy

Another important consideration is the management of email that resides on company messaging systems and your users’ computers. From the cost of storage and backup to legal and regulatory requirements, companies should document how they will handle email retention and implement basic controls to help them attain those standards.

Many industries have specific rules that dictate how long emails can or should be retained, but the basic rule of thumb is only as long as it supports your business efforts. Many companies implement a 60-90 day retention standard if not compelled by law to another retention period.

To ensure compliance, companies should consider mandatory archiving at a chosen retention cycle end date and automatic permanent email removal after another set point, such as180-360 days in archives. In addition, organizations should discourage the use of personal folders on employee computers (most often configurable from the e-mail system level), as this will make it more difficult to manage company standards.

Develop an email usage policy

Policies are important for setting expectations with your employees or users, and for developing standards to ensure adherence to your published polices.

Your policies should be easy to read, understand, define and enforce. Key areas to address include what the company email system should and should not be used for, and what data are allowed to be transmitted. Other policy areas should address retention, privacy and acceptable use.

Depending on your business and jurisdiction, you may have a need for email monitoring. The rights of the business and the user should be documented in the policy as well. The policy should be part of your general end user awareness training and reviewed for updates on a yearly basis.

Employees

(Federal-Communications-Commission-Small-Biz-Cyber-Security-Planning-Guide, 2012)

Businesses must establish formal recruitment and employment processes to control and preserve the quality of their employees. Many employers have learned the hard way that hiring someone with a criminal record, falsified credentials or undesirable background can create a legal and financial nightmare. Without exercising due diligence in hiring, employers run the risk of making unwise hiring choices that can lead to workplace violence, theft, embezzlement, lawsuits for negligent hiring and numerous other workplace problems.

Cyber Plan Action Items:

Develop a hiring process that properly vets candidates

The hiring process should be a collaborative effort among different groups of your organization, including recruitment, human resources, security, legal and management teams. It is important to have a solid application, resume, interview and reference-checking process to identify potential gaps and issues that may appear in a background check.

An online employment screening resource called the “Online Safe Hiring Certification Course” can help you set the groundwork for a safe recruitment process. The course will teach your teams what to look for in the different stages of the hiring process, how to interview and how to set up a safe hiring program to avoid hiring an employee that may be problematic. The course is available here: http://www.esrcheck.com/ESRonlineSafeHiringCourse.php.

Perform background checks and credentialing

Background checks are essential and must be consistent. Using a background screening company is highly recommended. The standard background screening should include the following checks:

- Employment verification
- Education verification
- Criminal records
- Drug testing
- The U.S. Treasury Office of Foreign Affairs and Control
- Sex offender registries
- Social Security traces and validation

Depending on the type of your business, other screening criteria may consist of credit check, civil checks and federal criminal checks. Conducting post-hire checks for all employees every two to three years, depending on your industry, is also recommended.

If you do conduct background checks, you as an employer have obligations under the Fair Credit Reporting Act.

For more information about employer obligations under the FCRA, visit: http://business.ftc.gov/documents/bus08-Using-consumer-reports-what-employers-need-know.

Take care in dealing with third parties

Employers should properly vet partner companies through which your organization hires third-party consultants. To ensure consistent screening criteria are enforced for third-party consultants, you need to explicitly set the credentialing requirements in your service agreement. State in the agreement that the company's credentialing requirements must be followed.

Set appropriate access controls for employees

Both client data and internal company data are considered confidential and need particular care when viewed, stored, used, transmitted or disposed. It is important to analyze the role of each employee and set data access control based upon the role. If a role does not require the employee to ever use sensitive data, the employee's access to the data should be strictly prohibited. However, if the role requires the employee to work with sensitive data, the level of access must be analyzed thoroughly and be assigned in a controlled and tiered manner following "least-privilege" principles, which allow the employee to only access data that is necessary to perform his or her job.

If the organization does not have a system in place to control data access, the following precautions are strongly recommended. Every employee should:

- Never access or view client data without a valid business reason. Access should be on a need-to-know basis.
- Never provide confidential data to anyone – client representatives, business partners or even other employees – unless you are sure of the identity and authority of that person.
- Never use client data for development, testing, training presentations or any purpose other than providing production service, client-specific testing or production diagnostics. Only properly sanitized data that cannot be traced to a client, client employee, customer or your organization's employee should be used for such purposes.
- Always use secure transmission methods such as secure email, secure file transfer (from application to application) and encrypted electronic media (e.g., CDs, USB drives or tapes).
- Always keep confidential data (hard copy and electronic) only as long as it is needed.
- Follow a "clean desk" policy, keeping workspaces uncluttered and securing sensitive documents so that confidential information does not get into the wrong hands.

- Always use only approved document disposal services or shred all hardcopy documents containing confidential information when finished using them. Similarly, use only approved methods that fully remove all data when disposing of, sending out for repair or preparing to reuse electronic media.

Provide security training for employees

Security awareness training teaches employees to understand system vulnerabilities and threats to business operations that are present when using a computer on a business network.

A strong IT security program must include training IT users on security policy, procedures and techniques, as well as the various management, operational and technical controls necessary and available to keep IT resources secure.

In addition, IT infrastructure managers must have the skills necessary to carry out their assigned duties effectively.

Failure to give attention to the area of security training puts an enterprise at great risk because security of business resources is as much a human issue as it is a technology issue.

Technology users are the largest audience in any organization and are the single most important group of people who can help to reduce unintentional errors and IT vulnerabilities. Users may include employees, contractors, foreign or domestic guest researchers, other personnel, visitors, guests and other collaborators or associates requiring access. Users must:

- Understand and comply with security policies and procedures.
- Be appropriately trained in the rules of behavior for the systems and applications to which they have access.
- Work with management to meet training needs.
- Keep software and applications updated with security patches.
- Be aware of actions they can take to better protect company information. These actions include: proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of security policy, and following rules established to avoid social engineering attacks and deter the spread of spam or viruses and worms.

A clear categorization of what is considered sensitive data versus non-sensitive data is also needed. Typically, the following data are considered sensitive information that should be handled with precaution:

- Government issued identification numbers (e.g., Social Security numbers, driver’s license numbers)
- Financial account information (bank account numbers, credit card numbers)
- Medical records
- Health insurance information
- Salary information
- Passwords

The training should cover security policies for all means of access and transmission methods, including secure databases, email, file transfer, encrypted electronic media and hard copies.

Employers should constantly emphasize the critical nature of data security. Regularly scheduled refresher training courses should be established in order to instill the data security culture of your organization. Additionally, distribute data privacy and security related news articles in your training, and send organization-wide communication on notable data privacy related news as reminders to your employees.

Implement Employee Departure Checklist

Create a security checkout checklist for employees that are no longer with your company, regardless of their reason for leaving (voluntary or involuntary). It's recommended by the U.S. Chamber of Commerce and others that all small businesses ensure terminated employee accounts are erased on all network devices and drives immediately.

This is especially true for any devices that may have been taken offsite such as laptops and smartphones.

Helpful links

- Stop.Think.Connect. Internal Employee Rollout Materials - http://www.dhs.gov/stopthinkconnect
- Internet Safety at Work PowerPoint Presentation - http://go.microsoft.com/?linkid=9745638
- Tip Cards: Top Tips for Internet Safety at Work - http://go.microsoft.com/?linkid=9745642
- Video: "Stay Sharp on Internet Safety at Work"- http://go.microsoft.com/?linkid=9745640
- U.S. Chamber of Commerce: Internet Security Essentials for Business 2.0 - https://www.uschamber.com/sites/default/files/issues/technology/files/ISEB-2.0-CyberSecurityGuide.pdf

Payment Cards

(Federal-Communications-Commission-Small-Biz-Cyber-Security-Planning-Guide, 2012)

If your business accepts payment by credit or debit cards, it is important to have security steps in place to ensure your customer information is safe. You also may have security obligations pursuant to agreements with your bank or payment services processor. These entities can help you prevent fraud. In addition, free resources and general security tips are available to learn how to keep sensitive information – beyond payment information – safe.

Cyber Plan Action Items:

Understand and catalog customer and card data you keep

- Make a list of the type of customer and card information you collect and keep – names, addresses, identification information, payment card numbers, magnetic stripe data, bank account details and Social Security numbers. It's not only card numbers criminals want; they're looking for all types of personal information, especially if it helps them commit identity fraud.
- Understand where you keep such information and how it is protected.
- Determine who has access to this data and if they need to have access.

Evaluate whether you need to keep all the data you store

- Once you know what information you collect and store, evaluate whether you really need to keep it. Often businesses may not realize they're logging or otherwise keeping unnecessary data until they conduct an audit.

Not keeping sensitive data in storage makes it harder for criminals to steal it.

- If you've been using card numbers for purposes other than payment transactions, such as a customer loyalty program, ask your merchant processor if you can use alternative data instead. Tokenization, for example, is technology that masks card numbers and replaces it with an alternate number that can't be used for fraud.

Use secure tools and services

- The payments industry maintains lists of hardware, software and service providers who have been validated against industry security requirements.
- Small businesses that use integrated payment systems, in which the card terminal is connected to a larger computer system, can check the list of validated payment applications to make sure any software they employ has been tested.

- Have a conversation about security with your provider if the products or services you are currently using are not on the lists.

Control access to payment systems

- Whether you use a more complicated payment system or a simple standalone terminal, make sure you carefully control access.
- Isolate payment systems from other, less secure programs, especially those connected to the Internet. For example, don't use the same computer to process payments and surf the Internet.
- Control or limit access to payment systems to only employees who need access.
- Make sure you use a secure system for remote access or eliminate remote access if you don't need it so that criminals cannot infiltrate your system from the Internet.

Use security tools and resources

Work with your bank or processor and ask about the anti-fraud measures, tools and services you can use to ensure criminals cannot use stolen card information at your business.

- For e-commerce retailers:
    - The CVV2 code is the three-digit number on the signature panel that can help verify that the customer has physical possession of the card and not just the account number.
    - Retailers can also use Address Verification Service to ensure the cardholder has provided the correct billing address associated with the account.
    - Services such as Verified by Visa prompt the cardholder to enter a personal password confirming their identity and providing an extra layer of protection.
- For brick and mortar retailers:
    - Swipe the card and get an electronic authorization for the transaction.
    - Check that the signature matches the card.
    - Ensure your payment terminal is secure and safe from tampering.

Remember the security basics

- Use strong, unique passwords and change them frequently.
- Use up-to-date firewall and anti-virus technologies.
- Do not click on suspicious links you may receive by email or encounter online.

Helpful links

You don't have to tackle security on your own. Work with your bank or processor to make sure you're getting the support and expertise you need.

- Visa offers a data security guide for small business as part of its Cardholder Information Security Program: http://usa.visa.com/download/merchants/uscc-cyber-security-guide-2012.pdf
- Information about industry security standards is available from the PCI Security Standards Council: https://www.pcisecuritystandards.org
- The Paysimple.com blog offers a helpful post on credit card security: http://paysimple.com/blog/2011/09/01/5-Tips-for-proper-handling-of-customer-credit-card-account-information/
- American Express provides data security advice for merchants: https://www260.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US
- MasterCard offers resources for on safeguarding customer information: http://www.mastercard.com/us/business/en/smallbiz/resources/industry/ecommerce/articles/0802CustomerData.html

Kiosks

(Maryland-Dept-of-Transportation-Information-Security-Plan, 2017)

The following standards should be followed whenever possible and if the facility can accommodate them.

Kiosk Operating System Security

- Password Protect the BIOS (8-character minimum, (larger when possible).
- Operating System should the latest possible release of Windows whenever possible.
- Operating System should auto-logon with a user account that has a password that adheres to the MDOT Security Policy for password complexity
- The Administrator account should be renamed.
- Block Internet access3, assign a static IP address to Kiosk and remove DNS.
- When business reasons call for internet access, the MDOT Change Process will be followed to assure the necessary mitigation takes place.
- Create a Kiosk user profile and augment with policy editor:
  1. Remove Run command from Start menu.
  2. Remove folders from Settings on Start menu.
  3. Remove Taskbar from Settings on Start menu.
  4. Remove Find command from Start menu.
  5. Hide drives on My Computer
  6. Hide Network Neighborhood
  7. Hide all items on Desktop
  8. Disable Shutdown Command
  9. Disable Registry Editing Tools

Kiosk Physical Security

- Configure switch port to only accept MAC address of Kiosk PC.
- Bolt Kiosk in place.
- Secure Kiosk access panels with commercial grade lock.
- Network cable should be placed in a conduit (ex. Greenfield) if the cable can't be run through the floor under the Kiosk.
- Network cable should be permanently attached to the jack or encased in a strong locked cover if it is accessible.
- Request the Kiosk to be placed in view of a security camera.
- A physical site assessment must be performed by the MDOT Information Security team before the kiosk is approved for production and public accessibility.

Internet Web Hosting Policy

(Maryland-Dept-of-Transportation-Information-Security-Plan, 2017)

Purpose

The purpose of this policy is to maximize the security of Web servers that are connected to the Internet and provide public information access. The focus is on the policies and procedures that must be in place to support any technical security features for the implementation and daily maintenance of Web servers. Without implementing proper security procedures, Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

Scope

This policy applies to all Internet Web server systems that are being built or in working condition regardless of whether they are hosted within MDOT or by a Third Party. Close attention should be made not only to the Web server itself, but also the security needs and requirements of the local network and other interconnected networks. In the case of collaborative efforts between MDOT and another governmental entity, MDOT management shall exercise due diligence to ensure that the intent of this policy is adhered to by the hosting party.

7.3 Policy Statement

There are many areas of Web servers to secure such as the underlying operating system, the Web server software, server scripts, and other associated components. All Agency Web servers that are accessible from the Internet must adhere to the following standards for operation and maintenance:

7.3.1 MDOT Hosting Policy:

1. Information placed on any Web site is subject to the same privacy restrictions as releasing non-electronic information. Accordingly, before information is placed on the Internet, it must be reviewed and approved for release in the same manner as other official memos, reports, or other official non-electronic information.
2. A public Web server must not serve as a repository for confidential data, although it can act as a proxy for access to confidential data located on more secure hosts.
3. Users are forbidden to download, install or run Web server software without prior approval by the user's Agency authorized system administrator.
4. Any control of Web servers must be done from the console or properly secured remote sessions by authorized administrators using encryption.
5. Web server software and the underlying operating system must employ all security patches and configuration options appropriate to the environment in which it is operating. Security patches must be maintained continually and all unnecessary services must be disabled.
6. Place Web servers on subnets separate from internal networks.
7. Firewalls and routers must be in place and configured to restrict attacks from public and internal networks as well. Only traffic needed for browsing and business applications management is allowed through the firewall to access that server.
8. Since using a computer simultaneously as a public Web server and for other public Web services poses risks, a computer must be dedicated to the sole function as a Web Server. Specifically, business or personal files are vulnerable to a malicious Web user if access is gained to a directory on your computer.
9. Keep the computer free of any networked or shared drives to another system. Access to remote machines opens an avenue for a malicious user to breach security.
10. Locate the computer in a physically secure area and restrict access to it by assigning passwords to authorized users. Ensure MDOT password policy is followed.
11. System administrators and security personnel must have defined responsibilities and authority to examine file systems on a regular basis for any unexpected changes. A review of logs on a regular basis by authorized personnel to record and report anomalies to your organization's designated security point of contact is desirable.

12. Procedures for Web server users to report any dramatically unexpected changes on the Web site to system administrators or your organization’s designated security point of contact must be in place.
13. An MDOT-approved Third Party will perform Web server security assessments bi-monthly unless unforeseen events require immediate assessment. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes (not page content), etc. The Modal COTR and/or IT Manager will be informed before the assessment is done and receive a copy of the results.

7.3.2 Third Party Hosting Policy:

MDOT hosting policies in sub-paragraphs 1, 2, 5, 7, 9, and 10 of paragraph 9.3.1 above also apply to Third Party Hosts. In addition, the following policies also apply:

1. Procedures for Web server users to report any dramatically unexpected changes on the Web site to system administrators or your organization’s designated security point of contact must be in place. The Third-Party Host must be able to take off-line any portion of the Website that has been compromised.
2. The State will contract a Third Party to perform Web server security assessments after the initial assessment, at the discretion of MDOT, unless unforeseen events require immediate assessment. The Third-Party Host will provide written authorization for MDOT to perform these security assessments as part of the original contract. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes, etc. The Modal COTR, IT Manager and Third-Party Host will be informed before the assessment is done and receive a copy of the results.
3. Non-compliance with policy directives may result in revocation of the Web Hosting contract. Additionally, MDOT content will be removed from the server and MDOT will retain the rights to the domain name.

7.4 Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement policy.

7.5 Guidance

This section establishes “high level” guidelines and standards supporting the agency policy. Guidelines are recommendations derived from best practices or experiences. Detail level implementing guidelines and procedures should not be included in the policy but should be contained in supporting documentation and referenced. Standards are mandatory requirements, which may be included in the policy text or supporting documentation and appropriately referenced. Electronic links must be provided whenever practical.

Agencies must consider addressing the following areas in the Guidelines section of their policy:

7.5.1 Security

Web server engineers or system administrators must not disclose any server structure or working information to any unauthorized personnel. All authorized personnel, whether State employees or Contractors, must sign a Non-Disclosure Agreement.

7.5.2 Records Retention

State Records communicated electronically must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system in accordance with each Department's standard practices. Retention of those records is the responsibility of the record owner.

Intranet Web Hosting Policy

(Maryland-Dept-of-Transportation-Information-Security-Plan, 2017)

Purpose

The purpose of this policy is to maximize the security of Web servers that are connected to an Intranet. The focus is on the policies and procedures that must be in place to support any technical security features for the implementation and daily maintenance of the Web servers. Without implementing proper security procedures, Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

Scope

This policy applies to all Intranet Web server systems that are being built or in working condition regardless of whether they are hosted within the MDOT or by a Third Party. Close attention is required for the Web server as well as the security needs and requirements of the Intranet since they frequently house sensitive corporate information not intended to be viewed by anyone outside the Agency. Intranets clearly illustrate how challenges to security are not so much technical as they are procedural.

Policy Statement

There are many areas of Web servers to secure including the underlying operating system, the server software, server scripts, and other associated components. Noteworthy, Intranets require strict internal security policies and procedures to control access to sensitive corporate data from within. Even though Intranet Web servers are not accessible from the Internet, they remain susceptible to the same attacks including penetrations from the Internet via other systems on the "inside network", and also through Internet Web browsing from the server. All Agency Web servers must adhere to the following standards for operation and maintenance:

1. Information placed on any site is subject to the same privacy restrictions when releasing non-electronic information. Accordingly, before information is place on the Intranet, it must be reviewed and approved for release in the same manner as other official memos, reports or other official non-electronic information.
2. Users must not run Web server software without prior approval by a user's Agency-authorized System Administrator.
3. Any control of Web servers must be done from the console or properly secured remote sessions by authorized administrators using encryption.
4. Server software and the underlying operating system must employ all security patches no later than one month of release and configuration options appropriate to the environment in

which it is operating. Security patches must be maintained continually and all unnecessary services must be disabled.

5. Locate the computer in a physically secure area and restrict access to it by assigning passwords to authorized users.
6. System administrators and security personnel must have defined responsibilities and authority to examine file systems on a regular basis for any unexpected changes. Additionally, authorized personnel must review logs regularly to record and report anomalies to your organization's designated Security Officer.
7. Procedures for Web Server users to report any dramatically unexpected changes on the site to system administrators or your organization's designated Security Officer must be in place.
8. A Third Party will perform Web server security assessments annually unless unforeseen events require immediate assessment. Also, security assessments must be accomplished after configuration changes such as operating system patches, web page script changes, etc. The Modal and/or IT Manager will be informed before the assessment is done and receive a copy of the results.

Responsibilities

Agency executive management will ensure that program unit management and unit supervisors implement policy.

Guidance

This section establishes "high level" guidelines and standards supporting the Agency policy. Guidelines are recommendations derived from best practices or experiences. Detail level implementing guidelines and procedures should not be included in the policy but should be contained in supporting documentation and referenced. Standards are mandatory requirements, which may be included in the policy text or supporting documentation and appropriately referenced. Electronic links must be provided whenever practical.

Agencies must consider addressing the following areas in the Guidelines section of their policy:

Security

Web server engineers or system administrators must not disclose any server structure or working information to any unauthorized personnel. All authorized personnel, whether State employees or Contractors, must sign a Non-Disclosure Agreement.

Records Retention

State Records communicated electronically must be identified, managed, protected and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system in accordance with each Department's standard practices. Retention of those records is the responsibility of the record owner.

Wireless Communications Policy

(Maryland-Dept-of-Transportation-Information-Security-Plan, 2017)

Purpose

The purpose of this document is to define a policy for securing wireless connections within MDOT's network. Due to the inherently insecure nature of this technology, only secure wireless systems that meet the requirements in this policy are approved for connection to the MDOT network. This policy is considered sensitive information and should not be shared outside of MDOT without the expressed written permission of the MDOT CIO.

Scope

This policy applies to all MDOT employees, and staff subordinate to MDOT contracts. It is recommended that the "Policy Statement" be included in any contract award process. This policy covers all wireless networking devices (e.g., Wireless Access Points, bridges, computing devices, etc.) connected to any of MDOT's internal networks. Wireless devices and/or networks without any connectivity to MDOT's networks do not fall under the purview of this policy.

Policy Statement

Computers and networks provide access to MDOT and remote resources, as well as the ability to communicate with other users worldwide. The security and integrity of this network must be upheld when utilizing wireless networking devices on the MDOT network.

In keeping with State of Maryland Department of Information Technology (DoIT) policy (Version 2.2) regarding Wireless (section 7.8), the following guidance will be observed:

- Establish a process for documenting all wireless access points
- Ensure proper security mechanisms are in place to prevent the theft, alteration. Or misuse of access points
- Restrict hardware implementation to utilize Wi-Fi certified devices that are configured to use the latest security features available
- Change default administrator credentials
- Change default SNMP strings if used, otherwise disable SNMP
- Change default SSID
- Deploy secure access point management protocols and disable telnet
- Strategically place and configure access points so that the SSID broadcast range does not exceed the physical perimeter of the building (unless the wireless solution is designed for providing outside connectivity).
- Require wireless users to provide unique authentication over encrypted channels if accessing internal LAN services
- Require wireless users to utilize encrypted data transmission if accessing internal LAN services

This MDOT/MDTA Wireless Communication Policy provides this additional guidance:

- No wireless access points shall be connected to the MDOT network without following the MDOT Change Management process.
- No end user device connected to the MDOT network (either wired or wireless) shall offer or allow connections to or from other networks
- No end user device will broadcast MDOT SSIDs or otherwise masquerade as a device providing connections to the MDOT network

- No MDOT wireless network management interfaces shall be accessible from the wireless network
- Wireless networks providing access to internal MDOT resources require WPA2 (Wi-Fi Protected Access - Enterprise) with two factor authentication.
- Wireless networks providing guest access to the Internet shall implement WEP (Wired Equivalent Privacy) at a minimum.
- Guest wireless network accounts will be unique and will be configured to expire passwords after eight hours. Exceptions to this policy must follow the MDOT Change Management process. For example, a one-week training class requiring guest wireless access may require an exception to the policy.

Responsibilities

Each Agency is responsible for developing procedure that is entirely consistent with this MDOT policy. The unique needs of each Agency's business and technical environments may include additional guidance as long as it is consistent with and meets the minimum requirements of MDOT policies, standards and guidelines. Agency executive management will ensure that program unit management and unit supervisors implement the policy.

Guidance

All wireless networking devices providing a wired connection to the MDOT network must have approval from the Security Working Group and be submitted for review via the Change Management process prior to being connected to the MDOT network. Due to the highly evolving nature of this technology, an MDOT Wireless Standards document (see Appendix D) will be kept on an on-going basis that contains current MDOT implementations of these technologies, known issues, and recommendations.

Wireless devices found to be non-compliant with this or other appropriate policies (i.e. Remote Access Policy, Email and Internet Use Policy) will have their connection terminated immediately.

ICS Cyber Security Program Activities

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

ICS Security Integration Group

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

The ICS Cyber Security program is highly dependent upon the expertise and participation of control system owners, engineers, and SMEs. As such, while the program is managed by Cyber Security, it is designed to work closely with ICS stakeholders. To help facilitate this, the ICS Security Integration Group was formed. This group is comprised of the following:

ICS Cybersecurity Steering Committee

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

A multifunctional team comprised of senior leaders and organization directors/managers whose purpose is to ensure excellent ICS Cybersecurity program performance is achieved and maintained. The ICS Cybersecurity Steering Committee typically meets quarterly to review program performance, determine program financial and personnel requirements, and approve reporting to be provided to the senior leadership team detailing the program's performance, deficiencies, and forward-looking activities.

ICS Cybersecurity Integration Committee

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

System owners, SMEs, mid-level managers, and information system security officers (ISSOs) whose purpose is to affect the design, operations, and maintenance of ICS, ensuring cybersecurity risks are mitigated in a cost-effective manner and comply with applicable regulations. The committee must place an emphasis on tailoring cybersecurity controls to meet safety, mission support/operations, and cybersecurity risk mitigation. The committee will strive for a balance between operational support and risk mitigation. The ICS Cybersecurity Integration Committee typical meets monthly to ensure program milestones, operational requirements, and cybersecurity risk mitigation metrics are being met.

ICS Cybersecurity Cross-Functional Team

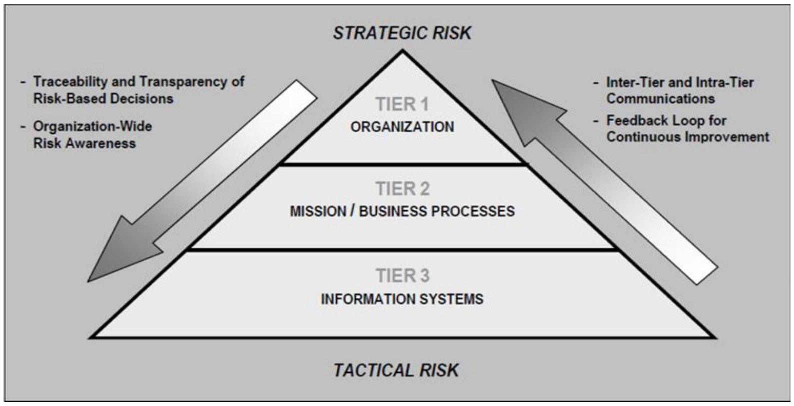
(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

A multidiscipline team consisting of system operators, maintenance personnel, engineers, Information Technology (IT) analysts, and/or cybersecurity analysts responsible for the routine design, operation, and maintenance of control systems. This team will be consulted on an as-needed basis (procedure/policy reviews, system assessments, design reviews, etc.), will be invited to participate in cybersecurity training opportunities, and should attempt to meet annually to share lessons learned, celebrate successes, and collaborate with peers.

Program Implementation Strategy

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

The ICS Cyber Security team has developed a strategy for applying the NIST Risk Management Framework to the many control systems. The proposed strategy is designed to approach this daunting task in a systematic manner that will help prioritize work activities and focus limited program resources. This strategy utilizes a tiered approach similar to that outlined by NIST's three-tiered risk management approach (**Error! Reference source not found.**).


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TACTICAL RISK

Program Implementation

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

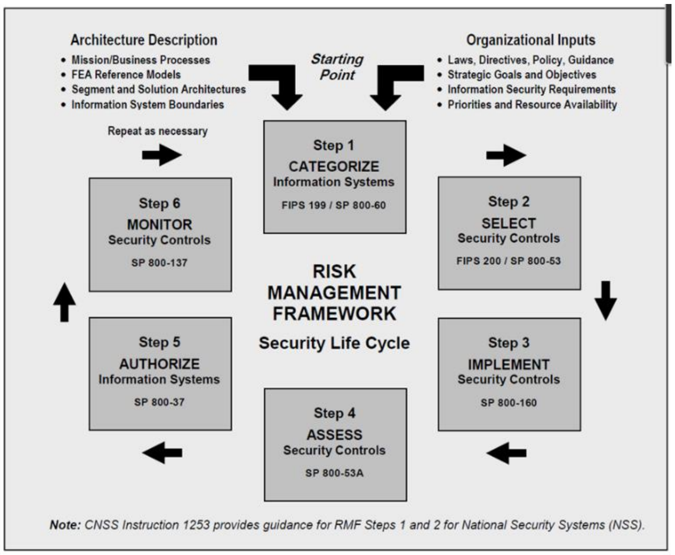
This is anticipated to be a multi-year effort, with initial efforts being focusing on Tier 1 and 2 activities, and future efforts working towards Tier 3 activities. The effort will continue until all ICS devices are inventoried and secured according to their respective system security plan (SSP). Tier 2 and Tier 3 activities will give priority to high-value INL assets first, as determined by the ICS Steering committees. Information identified in lower tiers, including the identification and/or mitigation of risks, will roll up to higher tier documents accordingly. System details from a Tier 3 activity, for instance, will be captured in the appropriate Tier 2 sub-enclave system security plan. Risks identified during a Tier 3 system assessment will be captured in a *Security Assessment Report* (see def.) and tracked/managed at the Tier 2 level. All outstanding risks will be reported up to the ATO at the Tier 1 level on an annual basis.

Program Implementation Workflow

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

NIST risk management framework

In addition to the steps listed in the NIST risk management framework recommend implementing a "Step 0," which consists of inventories of ICS assets and business impact assessments. Many of the ICSs make up core mission elements and are thus of high business importance and would have a significant impact if compromised.


Architecture Description
• Mission/Business Processes
• FEA Reference Models
• Segment and Solution Architectures
• Information System Boundaries
Starting Point
Organizational Inputs
• Laws, Directives, Policy, Guidance
• Strategic Goals and Objectives
• Information Security Requirements
• Priorities and Resource Availability
Repeat as necessary
Step 1 CATEGORIZE Information Systems FIPS 199 / SP 800-60
Step 6 MONITOR Security Controls SP 800-137
Step 2 SELECT Security Controls FIPS 200 / SP 800-53
RISK MANAGEMENT FRAMEWORK
Security Life Cycle
Step 5 AUTHORIZE Information Systems SP 800-37
Step 3 IMPLEMENT Security Controls SP 800-160
Step 4 ASSESS Security Controls SP 800-53A
Note: *CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).*

Existing/Legacy System Inventory

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

This section and the next section comprise "Step 0" mentioned earlier.

The inventory and initial assessment of existing/legacy ICS will be conducted in multiple phases.

An initial high-level inventory of existing/legacy major systems with their subcomponents will be collected. This inventory will be reported. These high-level inventories will be maintained within an inventory management system.

System owners or owning organizations will be responsible to ensure their ICS inventories are complete and accurate. This includes:

- Hardware
- Software/firmware
- Device configuration (see def.)
- Drawings (engineering and functional diagrams, including network topologies)
- Identification of network connections to the intranet or other networks
- Current identity and access management (clearance and badging) practices (including physical access restrictions)
- Current security administrative and technical controls in place and operational
- Current points of contact per system.

These detailed inventories will be maintained within the owning organizations inventory system and must be protected as highly sensitive information.

New Systems Inventory

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

Responsible/owning organizations implementing new or significantly modifying existing system must work with the ICS program Information System Security Manager (ISSM) to establish and implement the administrative and technical cybersecurity controls required to mitigate risks. New and existing systems undergoing significant modifications must ensure that their ICS inventories are complete and accurate. This includes:

- Hardware
- Software/firmware
- Device configuration
- Drawings
- Identification of network connections to the intranet or other network(s)
- Identity and access management practices
- Security administrative and technical controls.

Detailed inventories will be maintained within the owning organizations inventory system. The high-level summary inventory information will be maintained within an inventory management system.

Categorize System

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

Categorize system in accordance with FIPS-199 or a like model of categorization for security controls.

Utilizing the FIPS-199 information system categorization guidance, ICS assets will be categorized into major and minor assets. This categorization enables the use of a graded approach in the evaluation of INL control systems; major systems will incorporate dedicated SSPs with more comprehensive assessments, whereas minor systems will be covered under the broader SSP of the Special Systems Enclave and/or associated major system(s).

Based on guidance, FIPS-199 ratings for Availability (A), Integrity (I), and Confidentiality (C), will be established for each major system. The ratings will fall into the Low, Moderate, or High criteria of FIPS-199. The rating determines the level of standard mitigating controls (from NIST 800-53 and 800-82) that should be applied to the system. Risk assessments will then determine the residual risks to INL and DOE after mitigating controls are in place and shown to be effective.

An example of a minor system is a standalone microscope. The standalone microscope could be managed as part of a major system. Mission requirements and cost effectiveness should guide this decision.

Systems that perform a safety function must place emphasis upon maintaining health and safety controls with cybersecurity controls being of secondary importance

Security Controls

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

The initial set of controls for INL ICS will be selected and implemented according to NIST SP 800-82 and SP 800-53. All INL ICS systems must follow the guidance of these reference standards. The administrative and technical controls must be tailored to meet mission, safety, cost efficiency, operations, and security requirements specific to each system

Example - Assess

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

Initial Assessments

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

Initial assessment will be full scope in accordance with DOE O 205.1B, “Cyber Security Program,” and Energy program’s Risk Management Plan. The major system and associated subsystems will be assessed. The assessment standard will be NIST SP800-53 with 800-82 overlays. This includes the DOE’s Critical Security Controls.

Assessments will be prioritized and accomplished to meet mission support requirements. Cyber Security and mission organization personnel resources and the asset’s value will drive assessment schedules.

Conditions/Issues will be entered management incident and resolution tracking system.

Annual Assessments

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

Annual assessments will be conducted in accordance with DOE O 205.1B, “Cyber Security Program,” and Energy program’s Risk Management Plan. The scope of the assessments will vary include DOE’s Critical Security Controls. The assessment standard will be NIST SP 800-137 and SP 800-53 with SP 800-82 overlays for ICS.

As part of DOE’s continuous monitoring program, annual assessment of each major system and associated subsystems must be conducted. The annual assessments support the A&A processes. The annual assessments must:

- Review and determine status of the conditions/issues of the initial or previous year’s assessment
- Assess DOE’s critical security controls
- Assess the INL-established “Focus Area” controls. These controls are established each year by the Cyber Security department to address current threats and industry trends.

Ad-Hoc Assessments

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

Management assessments initiated in response to specific events, by request, in response to major system changes, or in response to newly identified risks/vulnerabilities may be conducted.

Assessment Response

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

Risks identified through independent audits, such as the annual Office of the Inspector General Financial System and General Support Systems Audit, Office of Enterprise Assessments, DOE-ID Assessments, and audits conducted internally via Internal Audits as part of the OMB Circular A123 audit will also be added to the unclassified *Plan of Actions and Milestones* (POA&M, see def.) Management System.

The POA&M document describes the actions taken or planned by the information system owner to correct deficiencies in the security controls and to address remaining vulnerabilities in the information system (that is, reduce, eliminate, or accept the vulnerabilities). The POA&M document identifies the tasks to be accomplished, the resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates.

Authorization

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

One of the primary goals of this program is to ensure that ICSs are assessed and authorized (A&A) in accordance with DOE O 205.1B, “Cyber Security Program.” This order requires adherence to the Nuclear Energy (NE) Risk Management Approach for cybersecurity. Classified and unclassified systems have been executing this Order and risk management approach since 2007. The intent for ICS assets is to include them in the existing DOE program/framework. This approach will allow the ICS program to join and leverage a mature cybersecurity risk management program.

Approach. For each sub-enclave this will include the designation of an ISSO to manage ICS assets and ensure that cybersecurity administrative and technical controls are operating as intended. This is a formal designation and must be part of the employee’s position description for both ISSM and ISSO.

All Employee Actions

Not Applicable

Instructions – Code of Conduct for Cyber Security Employees:

(INL-CyberSecurityOrganizationalGovernance, 2018)

Human Resources

(INL-CyberSecurityOrganizationalGovernance, 2018)

Cyber Security Employee: Annually perform a validation of the Skills Assessment to ensure gaps are understood. This information will be used as input into Individual Training Plans.

Manager/Lead: During the annual Performance Review process, review Position Description with the employee for accuracy and make any necessary changes.

Lead: Provide input to the Performance Review for the employees that work in their group. Leads may deliver and/or participate in the Performance Review interviews with employees that work in their group.

Manager: If at any time expectations of an employee are not being met, develop a written plan (i.e., Performance Improvement Plan [PIP]), or other appropriate human resource actions, to correct/improve performance.

Cyber Security Employee: Obtain approval from their Manager/Lead for personal leave (PL), compensation time, time-off without pay, or any other leave. This approval needs to be obtained prior to the leave being taken.

Cyber Security Employee: For issues with arriving to work for a regularly schedule shift or emergency leave, contact (phone, text, or e-mail) and provide status to the Manager/Lead.

Cyber Security Employee: As soon as plans are known, record on the Personal Leave calendar any time that will be spent away from the office. This includes PL, compensation time taken, working from home, travel, etc. 4.4.8 Cyber Security Employee: Designate a backup for essential functions during PL.

Cyber Security Employee: Prior to taking PL, hold a transition discussion to ensure the person who is filling in is prepared. When returning to work, hold a transition discussion with the fill-in to transfer critical information to maintain continuity.

Cyber Security Employee: Prior to taking PL, enable e-mail out of office settings, providing the leave and return dates, and who is the designated contact.

Cyber Security Employee: If needed, use the option of selecting start and stop times that allow an optimal work/life balance with prior management approval. Each work-day is expected to be 9 hours worked. No regular approved work schedule can start later than 9:00 a.m. or end earlier than 3:00 p.m. Employees must be available outside of their flexible schedule if requested by management. All exceptions must be communicated and approved by the Manager/Lead.

Cyber Security Employee: With prior Manager/Lead approval, use a flexible work week to accommodate work schedule using time billing system for exempt employees.

Architecture

(INL-CyberSecurityOrganizationalGovernance, 2018)

Cyber Security Architect: Create and maintain a Technology Roadmap for the organization. This is a living document which will be updated at least quarterly.

Cyber Security Architect: Hold quarterly architecture meetings within the Cyber Security organization to facilitate maintenance of the Technology Roadmap. This engagement allows for synergistic collaboration toward integrated, cohesive, and forward-looking technical solutions.

Cyber Security Architect: Feed the Technology Roadmap information into the Integrated Priority List, budget process, and asset maintenance plans including investments and divestments.

Safety

(INL-CyberSecurityOrganizationalGovernance, 2018)

Manager: On an annual basis, complete ergonomic assessments for every Cyber Security employee.

Manager: Whenever an employee moves from one office to another, perform an ergonomic assessment to ensure the employee’s workstation is set-up to be safe for the employee.

Cyber Security Employee: As a safety measure when working in the IORC building, keep office doors open when performing regular work so others can check on the well-being of their coworkers. If the need arises, use the status board outside the office to indicate if working in the office with the door closed.

Cyber Security Employee: Report all safety issues, concerns, or incidents to Manager/Lead as soon as reasonably possible.

Cyber Security Employee: As necessary, call a time out or stop work in accordance with LWP-14002, “Timeout and Stop Work Authority.”

Budget

(INL-CyberSecurityOrganizationalGovernance, 2018)

Manager: Use the Cyber Security budget to pay for Cyber Security personnel certifications if they are pertinent for an employee’s position.

Cyber Security: Discuss with manager which certifications are reimbursable.

Communication Expectations

(INL-CyberSecurityOrganizationalGovernance, 2018)

Cyber Security Employee: When representing the Cyber organization at a meeting, be vocal about all cybersecurity concerns relevant to the subject being discussed. Cyber Security staff is expected to, and have the right to, disagree and escalate all issues that may jeopardize cybersecurity posture or compliance.

Cellular Phone Stipend

(INL-CyberSecurityOrganizationalGovernance, 2018)

Cyber Security Employee: Provide a mobile phone number to be reached outside of working hours.

Managers/Leads: Due to the nature of the work in Cyber Security, obtain access to e-mail during off-work hours to deal with emergencies.

Manager: If it is deemed necessary for an employee to have access to e-mail at all times and they can show a financial burden to pay for the ability to access e-mail, establish a cellular phone stipend.
Manager: Review each cellular phone stipend annually to determine if it is still necessary.

Cyber Security Employee: If receiving a cellular phone stipend, publish cell phone number in the INL telephone directory.

Audit Governance

(INL-CyberSecurityOrganizationalGovernance, 2018)

NOTE: Cyber Security is audited on a regular basis. In many cases, much of the input for the audit comes from other organizations, in which case, Cyber Security plays a facilitative/coordination role.

Cyber Security Manager: For each audit, identify one point-of-contact.

Cyber Security Employee: Funnel all communications to auditing organizations through the main point-of-contact.

Cyber Security Audit Point of Contact: Ensure artifacts and documentation shared with external parties are protected as required

Cyber Security Audit Point of Contact: Escalate any findings

Governance, Risk and Compliance

(INL-UnclassifiedCyberSecurityProcedure, 2019)

Unclassified Cyber Security: Utilize *Governance, Risk, and Compliance (GRC)* process to maintain security control baselines, perform assessments, track security control compliance, identify cybersecurity gap issues, and document control implementations for INL systems and services.

Maintain the common and system-specific security controls baselines within GRC.

Document security control assessments procedures, results, and evidence in GRC.

Document security control gaps and risks.

Work with *Information System Owners* (see def.) and *Information System Security Officers* (ISSOs, see def.) to assist with the documentation of security control implementations as needed.

Security Control Assessment Process

(INL-UnclassifiedCyberSecurityProcedure, 2019)

Assessor(s): Perform the assessment using interviews, documentation reviews, observations, technical evaluations, and other tools. Record the assessment and supporting evidence within the GRC process.

Document assessment procedures and results for each security control. Where appropriate, include assessment evidence where possible (ISSOs may be leveraged to conduct tests, but the assessment result must be validated by the assessor prior to completion of the test).

Complete documentation of an issue in GRC process for failed controls tests. Full documentation of the issue following the procedures is necessary for each unique and notable issue. Where multiple control tests relate to an existing issue a simple reference to the issue is satisfactory.

Roles and Responsibilities

CIO

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

- Approves Cyber Security Program and is cognizant of the residual cyber risk
- Hires/appoints the CISO
- Establishes and maintains a framework to provide cybersecurity strategies aligned with business objectives consistent with applicable laws and regulations
- Approves cybersecurity policies
- Maintains laboratory-wide awareness of cybersecurity resources
- Advocates cybersecurity funding and personnel acquisition, as appropriate
- Acts as a laboratory spokesperson on cybersecurity issues
- Oversees the management of IT assets, including general support systems and major applications
- Ensures implementation of policies, procedures and guidelines to ensure effective planning, acquisition, secure operations and life-cycle management of IT assets in support of missions and objectives.

CISO

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

- CISO role Establishes, implements, and maintains Cyber Security Program to protect both classified and unclassified information assets.
- Information systems include specialized systems such as ICS, telephone switching systems (PBX), scientific instruments, and Environmental Management Systems (EMS).
- Develops and coordinates communication and implementation of cybersecurity policies and procedures
- Approves cybersecurity procedures and ensures their consistency with approved cybersecurity policies
- Manages risk profile and advises the Chief Information Officer, organizational directors, and senior leadership on significant cybersecurity threats and vulnerabilities
- Appoints the ICS ISSM
- Oversees the cybersecurity risk assessment and configuration management processes
- Formally characterizes residual cyber risk
- Identifies and assesses threats, vulnerabilities and asset value; and guides the implementation of protection measures
- Manages cybersecurity education and awareness training programs

- Human performance
- Manages a capability to respond to and recover from cybersecurity events
- Ensures cybersecurity incidents having potential counterintelligence ramifications are reported to the counterintelligence officer
- Reviews cybersecurity aspects of audits and inspections and is the liaison with DOE and outside agencies on issues involving cybersecurity audits and inspections
- Maintains appropriate cybersecurity files and records
- Coordinates requirements for the Cyber Security Program with laboratory personnel responsible for telecommunications security, operations security, physical security, and property management
- Leads cybersecurity audit preparation, finding response, and laboratory self-assessment processes
- Has authority to shut down systems or take any other action deemed necessary to protect laboratory computing and information assets.

ISSM

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

- ICS Cybersecurity program lead
- Appoints and oversees ICS ISSOs
- Leads ICS continuous monitoring program
- Primary liaison between CISO and ICS asset owners
- Ensuring the ICS cybersecurity program is compliant with departmental policy and the Senior Management Guidance
- Works with the CISO and acts as primary liaison for ICS cybersecurity
- Documents and monitors the ICS cybersecurity program
- Ensures Risk Management Approach is implemented for ICS cybersecurity resources
- Plans and budgets the ICS cybersecurity program
- Executes the Contractor Assurance System as applicable
- Establishes cybersecurity technical and administrative controls governing specialized systems such as ICS, telephone switching systems (PBX), scientific instrumentation, and Environmental Management Systems
- Ensures technical and administrative controls are implemented and remain effective for ICS
- Leads the ICS cybersecurity risk assessment and configuration management processes
- Leads ICS controls deviation/exception program
- Has working knowledge of ICS, system functions, cybersecurity policies, and technical cybersecurity protection measures.

ISSO

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

These individuals are responsible for ensuring that the appropriate operational security postures are maintained for ICS systems. The ISSO position is a functional position and typically is not in The Cyber Security organization or management chain. The responsibilities of this position include:

- Is the primary liaison between cybersecurity ICS ISSM and ICS asset owners
- Acts as the point of contact for the ICS regarding cybersecurity activities such as assessment and authorization, audits, reviews and inspections, and self-assessments

- Develops and maintains the ICS-specific supplement to System Security Plan documenting the security control implementation status and risk profile of the ICS
- Provides requested support for ICS-related cybersecurity incident response activities
- Consults with ISSM
- Maintains current inventory of ICS information assets and configurations
- Includes data inventory and detail configurations
- Has authority to shut down systems or takes any other action deemed necessary to protect laboratory computing and information assets.

ICS Owner

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

The following items for Information System Owner role include: industrial/process control systems, telephone switching systems, environmental management systems, scientific instruments, and other related systems.

- Ensures that assets within this area of responsibility adhere to all applicable cybersecurity policies and procedures
- Integrates and budgets for cybersecurity requirements throughout the life cycle of the asset
- Identifies ISSO (recommends to ISSM)
- Maintains management control of the configuration baseline of the asset, and ensures changes are coordinated via the established Configuration Management process
- Ensures that users and support personnel receive all required security training
- Ensures unique, asset-specific risks are reported to the business/mission manager, cybersecurity officer, and Performance Management Office.

ICS Users

- Understands and complies with policies
- Reports cybersecurity incidents in compliance with policies and incident response procedures
- Maintains cybersecurity awareness and protection of information and ICS assets under individual control.

Training

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

ICS personnel are trained to produce relevant and needed security skills and competencies by practitioners appropriate to their functional specialties and responsibilities. This is accomplished by education, experience, and professional training.

The INL ICS cybersecurity training program will be developed and maintain as a joint effort between the Cyber Security department and ICS asset owners. The Cyber Security department and ICS asset owners will contribute financial and full-time equivalent resources to ensure a high-quality and robust training program. The training program will focus on safety, human performance, ICS tampering detection and containment, and incident response.

The Cyber Security department and asset owner may partner with INL Training Department to create, deliver, and track training activities.

Human performance is a critical success factor within the ICS cybersecurity program. The training program must provide human performance testing with associated performance metrics. Annual human performance testing exercises must be conducted. Testing may be conducted in coordination with the site wide PLN-117, “Information Management Contingency Plan for Idaho National Laboratory,” exercises.

Staffing

(INL-IndustrialControlSystemCyberSecurityPlan, 2017)

The implementation strategy discussed above was used in conjunction with the current ICS asset list to provide a rough estimate of work hours required to perform the initial evaluation of existing INL control systems. The results of those estimates are displayed below

It should be noted that the above completion estimates address only the initial application of the first few steps of the Risk Management Framework, and only for existing control systems already in service at INL. Significantly more time and resources will be required to fully implement security controls and to implement long-term program tasks such as continuous monitoring training and awareness, procurement and design, and incident response and disaster recovery.

Other staffing will be needed to fully implement and maintain cyber security for INL ICS including ISSOs for each sub-enclave (see **Error! Reference source not found.**) as well as the overall ICS ISSO, and ICS ISSM. See sections **Error! Reference source not found.** and **Error! Reference source not found.**

Cyber Security Operations Manager

(INL-CyberSecurityProgramOperationsPlan, 2018)

- Functions as cybersecurity incident manager, activates the CSIRT, and directs all activities
- Makes operational decisions to contain and mitigate threats as deemed necessary to protect computing and information assets
- Is responsible for coordinating the technical implementation by all SMEs activated for the cybersecurity incident?
- Is responsible for maintaining a forensics-quality log of all events leading up to and during the cybersecurity incident including logs maintained by all team members during the cybersecurity incident
- Makes initial notifications to primary and secondary notification list personnel
- Obtains accurate ongoing accounting of events and provides updates to personnel on the primary notification list, as required
- Is responsible for completing reports and documentation during and after the cybersecurity incident.

Operations Technicians

(INL-CyberSecurityProgramOperationsPlan, 2018)

- Is responsible for investigating all events leading up to and during the cybersecurity incident
- Obtains accurate ongoing accounting of events and provides updates to the Cyber Security Operations Lead, as required
- Is responsible for completing reports and documentation at the completion of the cybersecurity incident
- Is responsible for completing after action reports.

Cyber Security Incident Response Team (CSIRT) Subject Matter Experts

(INL-CyberSecurityProgramOperationsPlan, 2018)

CSIRT SMEs are proficiently qualified within their areas of expertise. They should be fully trained on the CSIRT processes and are prepared to both directly implement changes as directed by CSIRT, as well as lead other members in their technical areas when necessary for larger cybersecurity incidents. There should be a primary and alternate SME for each of the following functional areas:

- Antivirus and Malware
- Network/Firewall
- Intrusion Detection System/Intrusion Prevention Systems
- OpsCenter (Call Center)
- E-mail and Collaboration Services
- Server Operations
- Desktop Management
- Managed Services (third-party contracted services)

Cyber Security Awareness Coordinator

(INL-CyberSecurityProgramOperationsPlan, 2018)

The Cyber Security Awareness Coordinator is responsible for training individuals on cybersecurity incident processes, completing after action reports of iJC3 reportable cybersecurity incidents, and conducting quarterly CSIRT exercises.

Extended Support roles

(INL-CyberSecurityProgramOperationsPlan, 2018)

During a cybersecurity incident, all communications with organizations external to IM will be channeled through the CISO. It is possible that CSIRT would need to interact with any organization. However, specific organizations have a greater likelihood of engagement during a cybersecurity incident. These organizations should assign a primary and alternate point of contact and these contacts should be familiar with CSIRT processes and have access to the CSIRT document. The organizations most likely to be engaged during a cybersecurity incident include:

- Information Security
- Legal
- Communications and Governmental Affairs
- Human Resources
- Physical Security
- Facility Management
- Counterintelligence
- Procurement
- Physical Security (Including Physical Security Officers)
- Freedom of Information/Privacy Act Officer

Information System Users

(INL-CyberSecurityProgramOperationsPlan, 2018)

Personnel who discover suspected or actual cyber security events are required to immediately report it to the Cyber Security Operations Center (CyberOps@'e-mail'), OpsCenter (Phone#) or Warning Communications Center (Phone#).

Cybersecurity Incident Life Cycle

(INL-CyberSecurityIncidentResponsePlan, 2019)

Detection

(INL-CyberSecurityIncidentResponsePlan, 2019)

Detection Incident Closure Containment / Mitigation Eradication / Restoration Preliminary Inquiry Notification / Reporting Declaration / Categorization

INL utilizes several mechanisms to identify cybersecurity incidents including:

- Cooperative Protection Project sensors located on the exterior of the network monitoring information traffic
- Notifications to the INL IM Operations Center by end users or other internal sources
- Notification from DOE's National Nuclear Security Administration's Information Assurance Response Center 24 × 7 Monitoring
- Reporting from antivirus, log aggregation, and network monitoring appliances
- Notifications (warnings and advisories) from various sources, including:
    - Federal Bureau of Investigation
    - iJC3
    - U.S. Computer Emergency Readiness Team
    - INL Counterintelligence
    - Non-government sources such as vendors or external sources.

Containment/Mitigation

(INL-CyberSecurityIncidentResponsePlan, 2019)

Containment and mitigation are important before a cybersecurity incident overwhelms resources or increases damage. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, or disable certain functions). The CISO will approve all strategies and risk acceptance during a cybersecurity incident.

All major services that are to be shut down or taken offline due to a cybersecurity incident must be approved by the director or their designee. All other services that must be shut down or taken off line shall be approved by the CISO or designee.

Preliminary Inquiry

(INL-CyberSecurityIncidentResponsePlan, 2019)

When a cybersecurity incident has occurred or is suspected to have occurred, a preliminary inquiry shall be conducted. The preliminary inquiry consists of gathering facts to determine and verify if a cybersecurity incident has occurred. Verbal interviews, gathering of potential evidence, and documentation of a cybersecurity incident should be conducted. Cyber Security will examine and document the pertinent facts and circumstances surrounding the event.

Cyber Security Operations has defined preliminary inquiry times based on the criticality of alerts received and potential functional impact. Cyber Security Operations team is not a supported 24×7 operation and the following time periods are all based on normal business hours.

1. **Critical** – Alert has the potential to impact all critical services to all system users. Response time: 4 hours.
2. **High** – Alert has the potential to impact all critical services to a subset of system users. Response time: 24 hours.

   Example: Information Assurance Response Center or notification, alerts that have been deemed actionable by the Advanced Cyber Capabilities Team, which can include phishing investigations, malware infections, Ops Center escalations or requests for investigations, and watch list notifications.

3. **Medium** – experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance. Response time: 24 hours.

   Example: Emerging threat rule Intrusion Detection System/Intrusion Prevention Systems and YARA rule alerts that were developed by the Advanced Cyber Capabilities team.

4. **Low** – experienced no loss in ability to provide all services to users. Response time: 1 week.

   Example: Routine investigations, alerts triggered by a single system that were developed by the Advanced Cyber Capabilities team.

If it is determined that a cybersecurity incident has occurred, the cybersecurity incident must be categorized according to the impact classifications, and reported within 1 hour.

Evaluations of cybersecurity incidents and potential cybersecurity incidents must be documented and local files retained.

If the Cyber Security Operations Manager determines a cybersecurity incident has not occurred, document inquiry, and no further action is necessary.

NOTE 1: *If the Cyber Security Operations Manager suspects or determines a violation of law has occurred, all inquiries must be halted and the Chief Information Security Officer and ISSM notified. If the inquiry establishes that a foreign power or an agent of a foreign power is involved, or involves a sensitive program, that is a significant risk to the environment than the Cyber Security Operations Manager must notify Chief Information Security Officer, ISSM, and CI.*

NOTE 2: *The responsibility for notifying appropriate federal, state, and local law enforcement belongs to the Chief Information Security Officer in coordination with Laboratory Protection, CI, and Executive Management.*

Cybersecurity Incident Types (Threat Vectors) – KB0013092

(INL-CyberSecurityIncidentResponsePlan, 2019)

Malicious Code: Instances of successful infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms, must be reported.

NOTE: *A minimum of 10 instances of successful infection or persistent attempts at infection within a 1-hour period by the same malicious code (e.g., viruses, Trojan horses, worms) must be reported.*

- **Loss, Theft, or Missing:** All instances of the loss of, theft of, or missing laptop computers; and all instances of the loss of, theft of, or missing information technology resources, including media that contained Controlled Unclassified Information (CUI) or national security information.

NOTE: *All instances of the loss of, theft of, or missing encrypted laptops, tablets, or media shall be treated as a property loss and not a data loss and reported in accordance with process x: "Lost, Stolen, or Damaged Government Property."*

- **Personally Identifiable Information (PII):** PII is any information collected or maintained about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.

NOTE: *Legal must be notified of any verified breach that results in the illegal acquisition of unencrypted computerized data that materially compromises the security of personal information in accordance with State Statute TITLE 28, Chapter 51, Section 104–107, "Identify Theft."*

- **Phishing:** The attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

NOTE 1: *A minimum of 10 successful phishing attempts within a 1-hour period or any phishing attempt considered significant by the ISSM must be reported.*

NOTE 2: *Successful attempt is defined as reaching a user's inbox allowing them the opportunity to interact with the malicious links or attachments of the e-mail.*

- **Attempted Intrusion:** A significant and/or persistent attempted intrusion is an exploit that stands out above the daily activity or noise level, as determined by the system owner, and would result in unauthorized access (compromise) if the system were not protected.
- **Classified Spillage:** Transfer of classified or sensitive information to unaccredited or unauthorized systems, individual's applications, or media. Spillage may result from improper handling of compartments, releasability controls, privacy data, or proprietary information.

NOTE: *All classified spillage incidents will be considered Incidents of Security Concern and will be responded to in accordance with plan x, Classified Information Spillage plan.*

- **Denial of Service:** Intentional or unintentional denial of service (successful or persistent attempts) that affects or threatens to affect a critical service or denies access to all or one or more large portions of a network, as determined by the system owner, must be reported. Critical services are determined through Business Impact Analyses in the Contingency Planning process.
- **Unauthorized Use:** Any activity that adversely affects an information systems normal, baseline performance, as determined by the system owner, and/or is not recognized as being related to business or mission is to be reported. Unauthorized use includes, but is not limited to, port scanning that excessively degrades performance; Internet Protocol spoofing; network reconnaissance; monitoring; hacking into servers; running traffic-generating applications that generate unnecessary network broadcast storms or drive large amounts of traffic; or using illegal

(or misusing copyrighted) software images, applications, data, and music. Unauthorized use can involve using systems to break the law.

Impact Classifications

(INL-CyberSecurityIncidentResponsePlan, 2019)

Functional Impact

- High – Organization has lost the ability to provide all critical services to all system users.
- Medium – Organization has lost the ability to provide a critical service to a subset of system users.
- Low – Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance.
- None – Organization has experienced no loss in ability to provide all services users.

Information Impact

- Classified – The confidentiality of classified information was compromised.
- Proprietary – The confidentiality of unclassified proprietary information, such as protected critical infrastructure information, intellectual property, or trade secrets was compromised.
- Privacy – The confidentiality of PII or personal health information was compromised.
- Integrity – The necessary integrity of information was modified without authorization.

Recoverability

- Regular – Time to recovery is predictable with existing resources.
- Supplemented – Time to recovery is predictable with additional resources.
- Extended – Time to recovery is unpredictable; additional resources and outside help are needed.
- Not Recoverable – Recovery from the cybersecurity incident is not possible (e.g., sensitive data exfiltrated and posted publicly).
- Not Applicable – Cybersecurity incident does not require recovery.
- None – No information was exfiltrated, modified, deleted, or otherwise compromised.

Cybersecurity Incident Declaration

(INL-CyberSecurityIncidentResponsePlan, 2019)

The CISO working with the ISSM and Cyber Security Operations Manager will declare all cybersecurity incidents. Upon declaration of a cybersecurity incident, the Cyber Security Operations Manager is authorized to activate the CSIRT team, including the requisition of assets and personnel to support the response process. The Cyber Security Operations Manager determines the appropriate level of response. All notifications are made at the discretion of the Cyber Security Operations Lead.

Cybersecurity Incident Reporting Process

(INL-CyberSecurityIncidentResponsePlan, 2019)

The CISO or designee must approve all external communications. All cybersecurity incidents shall be treated as CUI until reviewed by an Authorized Derivative Classifier. CSIRT communications between team members and external parties are to follow standard handling procedures for CUI information.

All cybersecurity incidents reported will be tracked and documented.

All cybersecurity incidents should be submitted through a web-based cybersecurity incident submission form

If required, information sent by e-mail should be protected with encryption.

Send e-mail describing the cybersecurity incident to ……

If the cybersecurity incident requires priority handling, use the phrase "URGENT" in the e-mail subject line and an analyst will contact the sender.

If a cybersecurity incident requires immediate attention, contact the Call Center at xxx-xxx-xxxx, where an analyst is available 24/7/365. Please restrict the non-business hour's use of the Call Center to emergency situations.

Eradication/Restoration

(INL-CyberSecurityIncidentResponsePlan, 2019)

After a cybersecurity incident has been contained, eradication may be necessary to eliminate components of the cybersecurity incident (e.g., deleting malware, disabling breached user accounts, identifying and mitigating all vulnerabilities that were exploited). During eradication, it is important to identify and document all affected hosts so they can be remediated. For some cybersecurity incidents, eradication is either not necessary or is performed during restoration.

During restoration, system administrators shall document and restore systems to normal operation, confirm that the systems are functioning normally, and, if applicable, remediate vulnerabilities to prevent similar cybersecurity incidents. Restoration may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists). Instituting higher levels of system logging or network monitoring are often part of the recovery process.

Cybersecurity Incident Closure

(INL-CyberSecurityIncidentResponsePlan, 2019)

A final report must be completed documenting the pertinent facts and circumstances surrounding the event after a cybersecurity incident is officially closed.

All "lessons learned" for cybersecurity incidents reported will be tracked and documented. After the cybersecurity incident has been resolved, users shall receive a post cybersecurity incident questionnaire.

Any necessary adjustments to the cybersecurity program will be evaluated based on the post cybersecurity incident review.

Cybersecurity Alerts and Cybersecurity Emergencies

(INL-CyberSecurityIncidentResponsePlan, 2019)

- CISO shall respond promptly to actionable cybersecurity emergency declarations, analyzing threat information, and performing corrective/preventive actions as required.
- As a minimum, shall:
- Acknowledge actionable alerts and emergencies.

- Execute analyses relative to the activities described in the alert or cybersecurity emergency declaration.
- Execute appropriate corrective/preventive actions.
- Report the actions taken or provide justification for actions not taken.

Cybersecurity Incident Tracking

(INL-CyberSecurityIncidentResponsePlan, 2019)

All potential cybersecurity incident inquiries and reportable cybersecurity incidents must be documented and local files retained.

CSIRT incidents will be tracked in a security incident log area. All unclassified cybersecurity incidents shall be recorded and objective evidence uploaded to this area.

Measuring CSIRT Effectiveness

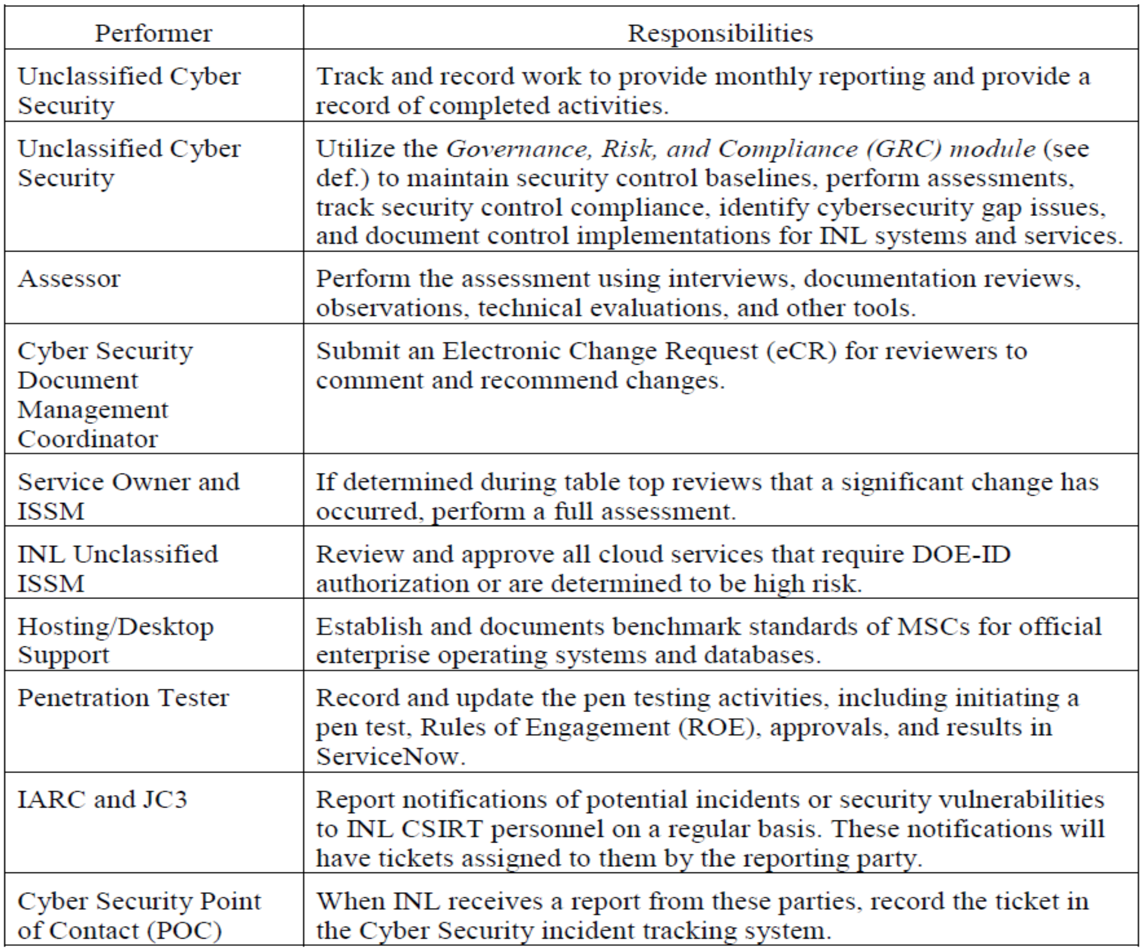
Using the CSIRT tracking system, the following metrics will be available to measure the effectiveness of the CSIRT program.

- Number of cybersecurity incidents handled (quantitative metric).
- Time between event detection and cybersecurity incident declaration (quantitative metric).
- Time between cybersecurity incident declaration and cybersecurity incident closure (quantitative metric).
- Lessons learned (qualitative metric – provided by individual CSIRT members).

Appendix A, Major Systems and Subsystems Initial Inventory

Appendix B, Responsibilities

(INL-UnclassifiedCyberSecurityProcedure, 2019)



Performer	Responsibilities
Unclassified Cyber Security	Track and record work to provide monthly reporting and provide a record of completed activities.
Unclassified Cyber Security	Utilize the *Governance, Risk, and Compliance (GRC) module* (see def.) to maintain security control baselines, perform assessments, track security control compliance, identify cybersecurity gap issues, and document control implementations for INL systems and services.
Assessor	Perform the assessment using interviews, documentation reviews, observations, technical evaluations, and other tools.
Cyber Security Document Management Coordinator	Submit an Electronic Change Request (eCR) for reviewers to comment and recommend changes.
Service Owner and ISSM	If determined during table top reviews that a significant change has occurred, perform a full assessment.
INL Unclassified ISSM	Review and approve all cloud services that require DOE-ID authorization or are determined to be high risk.
Hosting/Desktop Support	Establish and documents benchmark standards of MSCs for official enterprise operating systems and databases.
Penetration Tester	Record and update the pen testing activities, including initiating a pen test, Rules of Engagement (ROE), approvals, and results in ServiceNow.
IARC and JC3	Report notifications of potential incidents or security vulnerabilities to INL CSIRT personnel on a regular basis. These notifications will have tickets assigned to them by the reporting party.
Cyber Security Point of Contact (POC)	When INL receives a report from these parties, record the ticket in the Cyber Security incident tracking system.

Glossary

Acronyms

References

AmericanWaterWorksAssocationCyberSecurityTool. (2014). *AWWACyberSecurityTool.* Denver, CO: American Water Works Association.

AmericanWaterWorksAssociationCyberSecurityAssessementAndRecommendedApproach. (2016). *Cyber Security Assessment and Recommended Approach, Appendix B.* Delaware: State of Delaware Drinking Water Systems Final Report; KashSrinivasanGroup-DelewareDrinkingWaterSystem.

AmericanWaterWorksAssociationCyberSecurityTool. (2014). *American Water Works Associatiton Cyber Security Tool.* TBD: AmericanWaterWorksAssociation.

A-Threat-Driven-Approach-To-Cyber-Security-2019-Muckin&Fitch. (2019). *A Threat Driven Approach to Cyber Security, Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization.* Lockheed Martin Corporation.

Cyber-Security-Planning-Guide-NewYork-Small-Business-Development-Center. (2016). *Cyber-Security-Planning-Guide.* Albany, New Yokr: New Yorks Small Business Development Center/partial funds by United States Small Business Development Center; State University of New York.

CyberSecurityPolicyDocumentforManagers. (2016). *Cyber Security Policy Document for Managers.* Deleware: State of Delaware Drinking Water Systems Final Report; KashSrinivasanGroup-DelewareDrinkingWaterSystem.

Department-of-Homeland-Security-Cyber-Resilience-Review-CRR-Self-Assessment-Package. (2016). *Department-of-Homeland-Security-Cyber-Resilience-Review-CRR-Self-Assessment-Package.* Pittsburgh, Pennsylvania: Carnegie Mellon University Software Institute.

Federal-Communications-Commission-Small-Biz-Cyber-Security-Planning-Guide. (2012). *FCC -Cyber Security Planning Guide.* Columbia, Maryland: Federal Communications Commission.

GuidetoIndustrialControlSystems(ICS)Security-Stouffer, P. (2015). *Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2.* Gaithersburg, Maryland: National Institute of Standards and Technology Special Publication 800-82 http://dx.doi.org/10.6028/NIST.SP.800-82r2 CODEN: NSPUE2.

Handbook-for-Self-Assessing_Security_Vulnerabilities&Risks_of_Industrial_Control_Systems_on_DOD_Installations. (2012). *Handbook-for-Self-Assessing_Security_Vulnerabilities&Risks_of_Industrial_Control_Systems_on_DOD_Installations.* Pentagon, Virginia: Operational Test and Evaluation, Office of Secretary of Defense;Joint Threat Assessment and Negation for Installation Infrastructure Control Systems (JITANIICS);Quick Reaction Test(QRT);;Joint Test and Evaluation (JT&E);.

Information-Security-Plan-Template-State-of-South-Carolina. (2013). *Information-Security-Plan-Template-State-of-South-Carolina.* Colombia, South Carolina: State of South Carolina.

INL-CyberSecurityIncidentResponsePlan. (2019). *Idaho National Laboratory Cyber Security Incident Response Plan.* Idaho Falls, Idaho: Idaho National Laboratory.

INL-CyberSecurityOrganizationalGovernance. (2018). *Cyber Security Organizational Governance.* Idaho Falls, Idaho: Idaho National Laboratory.

INL-CyberSecurityProgramOperationsPlan. (2018). *Cyber Security Program Operations Plan.* Idaho Falls, Idaho: Idaho National Laboratory.

INL-IndustrialControlSystemCyberSecurityPlan. (2017). *Industrial Control System Cyber Security Plan* . Idaho Falls, Idaho: Idaho National Laboratory .

INL-UnclassifiedCyberSecurityProcedure. (2019). *Idaho National Laboratory-UnclassifiedCyberSecurityProcedure.* Idaho Falls, Idaho: Idaho National Laboratory.

Maryland-Dept-of-Transportation-Information-Security-Plan. (2017). *Maryland Department of Transportation Information Security Plan.* Annapolis, Maryland: State of Maryland.

New-York-State-Information-Security-plan-template-Defense-Counterintelligence-and-Security-Agency. (2018). *The Defense Counterintelligence and Security Agency;Election Infrastructure ISAC.* East Greenbush, New York: New York State Cyber Security Plan Tool Kit.

NIST-800-161-SupplyChainRiskmanagementpracticesforFederalInformationSystemsandorganizations. (2015). *NIST-800-161-SupplyChainRiskmanagementpracticesforFederalInformationSystemsandorganizatio.* Gaithersburg, Maryland: National Institue of Standards and Technology; Department of Commerce.

NIST-800-94-GuidetoIntrusionDetectionandPreventionSystems. (2007). *GuidetoIntrusionDetectionandPreventionSystems.* Gaihersburg, Maryland: National Institute of Standards and Technology.

NIST-GuideforConductingRiskAssessments-800-30-R1. (2012). *NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments.* Gaithersburg, Maryland: National Institute of Standards and Technology U.S. Department of Commerce.

NISTIR8179-Criticality-Analysis-Process-Model-Prioritizing-Systems-and-Components. (2017). *NIST IR 8179 Criticality Analysis Process Model Prioritizing Systems and Components.* Gaithersburg, Maryland: National Instute of Standards and Technology.

NIST-Managing-Information-Security-Risk-800-39. (2011). *NIST Special Publication 800-39: Organization, Mission, and Information System View.* 2011: National Institute of Standards and Technology U.S. Department of Commmerce.

NRECAGuidetoDevelopingaCyberSecurityandRiskMitigationPlan. (2011). *Guide to Developing a Cyber Security and Risk Mitigation Plan.* Arlington, Virginia: National Rural Electric Cooperative Association (NRECA); Prepared by Evgeny Lebanidze Cigital 21351 Ridgetop Circle Suite 400 Dulles, VA 20166-6503.

Physical_Security_Plan-Center-for-Development-of-Security-Excellence. (2013). *Physical_Security_Plan-Center-for-Development-of-Security-Excellence.* Quantico, Virginia: Center for Development of Security Excellence; Defense Counterintelligence and Security Agency.

State-of-Maryland-IT-Department-Security-Incident-Management-Plan. (2017). *Security Incident Management Plan version 008.* Annapolis, Maryland: Maryland.

United-States-Nuclear-Regulatory-Commission-Part73-Cyber-Security-Plan-Implementation-Schedule. (2018). *Title 10 of the Code of Federal Regulations, Part 73, "Physical Protection of Plants and Materials," Section 73.54, "Protection of Digital Computer and Communication Systems and Networks,".* Rockville, Maryland: United States Nuclear Regulatory Commission.

University-of-Southern_Florida_IT-Security_Plan. (2019). *University-of-Southern_Florida_IT-Security_Plan.* Tampa, Florida: University of Southern Florida.