INSPECTION MANUAL CHAPTER 0609, APPENDIX E, PART IV

CYBERSECURITY SIGNIFICANCE DETERMINATION PROCESS FOR POWER REACTORS

Effective Date: 05/18/2026

PROGRAM APPLICABILITY: IMC 2201 A

CORNERSTONES: Security

0609EIV-01 PURPOSE

The purpose of the cybersecurity significance determination process (SDP) is to provide an objective means of evaluating performance deficiencies relating to cybersecurity requirements for power reactors licensed by the U.S. Nuclear Regulatory Commission (NRC).

01.01 More-than-Minor Process Overview. The process for determining if a performance deficiency is minor or more-than minor is depicted in Figure 1, “Minor vs More-than-Minor Determination.”

01.02 Cybersecurity Significance Determination Process Overview. The process for determining the significance of a performance deficiency, and the criteria to be used in the analysis of the finding, is depicted in Figure 2, “Starting Point for Finding Significance Determination.”

01.03 Determination Process for an Actual Cyberattack. If the performance deficiency is associated with an actual cyberattack that did have an adverse impact to a safety, important to safety, security, or emergency preparedness (SSEP) function(s), then the significance should be determined by utilizing either Figure 3, 4, or 5, depending on the impacted SSEP function.

01.04 Significance Screen. The significance screen process depicted in Figure 2 includes four steps in which the inspector(s) should identify if the deficiency would enable an adverse impact to an SSEP function by way of a cyberattack. If the deficiency would not enable an adverse impact to an SSEP function by way of a cyberattack, as determined in the four screening steps, then the deficiency should be assessed as very low significance. If the deficiency would enable an adverse impact to an SSEP function by way of a cyberattack, then the significance should be determined by using the respective processes depicted in either Figure 3, 4, or 5 depending on the SSEP function at risk.

0609EIV-02 BACKGROUND

Evaluating the Finding

The cybersecurity events of the twenty-first century (e.g., Stuxnet) have changed the cybersecurity environment. An important element of objectives to be faced in cybersecurity

protection prioritization relates to the evolution of the cybersecurity threat environment. Cybersecurity is a dynamic arena as shifts in threat actor capabilities occur.

In order to accommodate such evolutionary changes, this cybersecurity SDP focuses on the primary concern: Does the licensee's existing cybersecurity plan (CSP) and cybersecurity program provide adequate protection against cyberattacks? If current conditions provide a potential attacker with a pathway that can be used to access an asset, if the asset has exploitable cybersecurity vulnerabilities, and if the licensee has inadequate ability to detect and stop an attack, the likelihood of adverse impact to an SSEP function is increased.

0609EIV-03 DEFINITIONS

Adverse Impact

A direct deleterious effect on a critical digital asset (CDA) (e.g., loss or impairment of function; reduction in reliability; reduction in ability to detect, delay, assess, or respond to malevolent activities; reduction of ability to call for or communicate with offsite assistance; and the reduction in emergency response ability to implement appropriate protective measures in the event of a radiological emergency). In the case where the direct or indirect compromise of a support system causes an SSEP or support system to actuate or "fail safe" and not result in radiological sabotage (i.e., causes the system to actuate properly in response to established parameters and thresholds), this is not considered to be an adverse impact as it is defined by Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54(a) (Regulatory Guide (RG) 5.71).

Cyberattack

The manifestation of either physical or logical (i.e., electronic or digital) threats against computers, communication systems, or networks that may: (1) originate from either inside or outside the licensee's facility; (2) have internal or external components; (3) involve physical or logical threats; (4) be directed or non-directed in nature; (5) be conducted by threat agents having either malicious or non-malicious intent; and (6) have the potential to result in direct or indirect adverse effects or consequences to CDAs or critical systems (CSs). This includes attempts to gain unauthorized access to a CDA and/or CS's services, resources, or information; the attempt to compromise a CDA and/or CSs integrity, availability, or confidentiality; or the attempt to cause an adverse impact to an SSEP function. Further background on cyberattacks up to and including design basis threat, can be found in Regulatory Guide 5.69, "Guidance for the Application of the Radiological Design-Basis Threat in the Design, Development, and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements," and the licensee's cybersecurity plan (CSP) (RG 5.71).

Cybersecurity Vulnerability

A feature, attribute or weakness in a system's design, implementation, or operation and management that could render a CDA open to exploitation or SSEP function susceptible to adverse impact (RG 5.71).

Human-Machine Interface (HMI)

The peripheral devices utilized by a computer or intelligent device that provide a means for human interaction with the computer/device via some form of data display and/or data input mechanism.

Initiating Event

The plant system perturbations to the steady state of the plant that challenge plant control and safety systems whose failure could lead to core damage and or radioactivity release. These initiating events include failure of equipment from either internal plant causes (such as hardware faults, operator actions, floods, or fires), or external plant causes (such as earthquakes or high winds). Cyberattacks, depending on their nature, could be considered either an internal or external cause. (See RG 1.200 “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities.”)

Plant Transient

A departure from equilibrium or steady-state operations characterized by either a thermal or reactivity imbalance.

Plant Trip

The shutdown of the reactor by the rapid addition of negative reactivity by any means, (e.g., insertion of control rods, boron, use of diverse scram switch, or opening reactor trip breakers). Synonymous with a reactor scram.

Risk Significant System

A plant system that is categorized as high risk significant (or high safety significance) by the utility’s Maintenance Rule Program in accordance with 10 CFR 50.65, to include spent fuel pool cooling and inventory systems.

Zero Day Attack

A cyberattack that exploits a previously unknown cybersecurity vulnerability, meaning that the attack occurs on "day zero" of awareness of the cybersecurity vulnerability. This means that the developers and users have had zero days to address and patch the cybersecurity vulnerability.

0609EIV-04 REQUIREMENTS

04.01 Entry Conditions – Initial Inspector Review

When the inspector has a potential issue, before entering the cybersecurity SDP, the issue should be screened using Inspection Manual Chapter (IMC) 0612, Appendix B, "Issue Screening,” to determine if there is a performance deficiency. If a deficiency is identified, the inspector should consult IMC 0609, Attachment 4, “Initial Characterization of Performance Deficiencies,” to determine the applicable cornerstone. If the “Security Cornerstone” is confirmed, the inspector should proceed to IMC 0609, Appendix E, “Security Significance Determination Process for Power Reactors.” If the issue is determined to be a cyber-related performance deficiency, the inspector should then refer to IMC 0609, Appendix E, Part IV, “Cybersecurity Significance Determination Process for Power Reactors,” and inspectors should enter the minor versus more-than-Minor analysis at the top of Figure 1, IMC 0609 Appendix E, Part IV.

04.02 Entry Conditions – Findings with Multiple Examples

When characterizing a finding, multiple individual performance deficiencies cannot be aggregated into one finding of greater significance. Additionally, if a finding has multiple occurrences (e.g., a consistent incorrect security policy setting in multiple CDAs), the most significant example should be used to characterize the overall significance of the finding. Similarly, if a given finding impacts multiple SSEP functions, then the most significant impact should be used to characterize the overall significance of the finding(s). If a finding involves protection of safeguards information (SGI), the significance will be determined using IMC 0609 Appendix E Part I, "Baseline Security Significance Determination Process for Power Reactors." If the inspectors(s) have both cybersecurity and SGI related findings, Appendix E Part I and Part IV will be used to assess the respective findings.

04.03 Determining Minor Cybersecurity Findings

If there is a performance deficiency, then the inspector must determine if the performance deficiency is more-than-Minor. Answer the following questions to determine if the PD is more-than-Minor.

a. Degraded, Failure, or Missing Cybersecurity Control

Question A.1: Did the PD result in a degradation, failure, or missing cybersecurity control?

a. If YES ➛ Go to Question A.2.
b. If NO, continue to Section b, Counter Measures.

Question A.2: Was there a substantive[1] decrease in the CDAs defense-in-depth protections?

a. If YES ➛ The PD is more-than-minor. Go to Figure 2, Starting Point for Finding Cybersecurity Significance Determination.
b. If NO, go to Section b, Counter Measures.

---

[1] These are examples of substantive decrease in defense-in-depth protections. This is not an exhaustive list but can be used by inspectors to support the minor vs more-than-Minor assessment.

1. Resetting Passwords - A substantive decrease in defense-in-depth would occur if the licensee failed to update any passwords across multiple critical digital asset (CDA) within the required periodicity, or if a single CDA's password was missed for multiple update cycles. In contrast, the issue would likely be considered minor if the licensee had an established password management program in place and only one or two CDA passwords were missed during a single cycle. It would also be minor if the licensee provided an adequate evaluation that demonstrated alternate controls were shown to mitigate the threat/attack vector.
2. Degraded Control on a Protection CDA - Failure to adequately implement required control(s) on a device that is relied upon by multiple CDAs is a substantive decrease in defense in depth. Failure to have required policies and procedures, failure to follow policies and procedures, are a substantive decrease in defense-in-depth. These devices include boundary devices (e.g., data diode, firewall), monitoring devices (e.g., SIEM, IDS, HIDS, NIDS), and anti-virus systems. Footnote 3 also applies to protection CDAs and if an appropriate evaluation finds that the vulnerability doesn't need to be remediated, it is not substantive.
3. Vulnerability Management - A substantive decrease in defense in depth occurs when a licensee fails to evaluate or address a vulnerability and the vulnerability would require remediation. If an appropriate evaluation finds that the vulnerability doesn't need to be remediated, it is not substantive.

b. Counter Measures

Question B.1: Did the PD result in the need for counter measures to mitigate the attack vector that the security control was designed to protect?

a. If YES ➛ Go to Question B.2.
b. If NO, continue to Section c, Multiple Failures.

Question B.2: Were the counter measures not implemented or insufficient to mitigate the associated risk?

a. If YES ➛ The PD is more-than-minor. Go to Figure 2, Starting Point for Finding Cybersecurity Significance Determination.
b. If NO, go to Section c, Multiple Failures.

c. Multiple Failures

Question C.1: Did the PD result in failure of multiple controls impacting a single CDA?

a. If YES ➛ Go to Question C.3.
b. If NO ➛ Go to Question C.2.

Question C.2: Did the PD include the failure of a single control that impacted multiple CDAs (IDS, IPS, SIEM, Time Server, etc.)?

a. If YES ➛ Go to Question C.3.
b. If NO ➛ The PD is minor.

Question C.3: Does the licensee have measures in place that substantially mitigate the impact?

a. If YES ➛ The PD is minor.
b. If NO ➛ The PD is more-than-minor. Go to Figure 2, Starting Point for Finding Cybersecurity Significance Determination.

04.04 Evaluating the Finding

Does the finding involve an actual cyberattack that adversely impacted an SSEP function? If a cyberattack did adversely impact an SSEP function, then the SDP will proceed immediately to either:

Figure 3, if the impact was to a safety, safety-related, or important to safety function or;

Figure 4, if the impact was to a physical security function or;

Figure 5, if the impact was to an emergency preparedness (EP) function.

04.05 The primary concern in assessing the significance of a finding associated with the licensee's cybersecurity program, is determining if the identified deficiency would enable a cyberattack on a CDA that would result in an adverse impact to an SSEP function. There are four steps involved in establishing that condition. The following steps will enable the inspector(s) to determine the significance of the finding. To assist inspector(s)

in evaluating the finding, the guidance in paragraphs 04.06-04.09 provide additional details on timely detection, response, and mitigation before adverse impact, that is lacking in NRC Regulatory Guide (RG) 5.71 and Nuclear Energy Institute (NEI) 08-09. This guidance has been derived from NRC, NEI, Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST) sources. If, however, the licensee uses an NEI guidance document that provides detailed guidance concerning timely detection, response, and mitigation before adverse impact and that guidance found acceptable for use by the NRC, inspector(s) shall use that guidance to evaluate the finding.

04.06 Step 1 – Identification of Attack Pathway to Critical Digital Asset

Requirements in 10 CFR 73.54 (the rule), and the CSP such as hardening, defense in depth, and many other security measures and controls, if implemented effectively by the licensee, should eliminate an attack pathway. If the following questions are answered in the negative, then the process is complete and the inspector should conclude that the finding is of very low significance. If any produce a “yes” response, then there is a pathway that could be used to stage a cyberattack on a CS/CDA. In that case the inspector should proceed to the next phase of verification, 04.07 Step 2 - identification of exploitable cybersecurity vulnerabilities.

a. Physical Access to the CDA

Is physical access to, and manipulation of, the CS/CDA or use of the CS/CDA’s HMI possible by personnel other than those with access authorization?

b. Supply chain access to the CDA

Are vendor-provided software patches and updates installed without prior validation and testing on a separate support system or test bed contrary to the licensee’s CSP?

Is the CS/CDA vendor permitted to have remote access to the CS/CDA for support purposes without cyber and physical end-point security?

Are there any system and services acquisition requirements that have not been implemented in accordance with the licensee’s CSP?

c. Portable media/device connectivity to the CDA

Can any form or format of portable electronic storage media be connected to (or mounted on a media drive) and utilized by the CS/CDA?

Can any form of portable computer/intelligent device be connected to and intercommunicate with the CS/CDA?

d. Wired communications with the CDA

Does the CS/CDA have an enabled communications adapter with a connection to any type of local area network (LAN) or wide area network (WAN)?

Does the CS/CDA have an internal or external modem with a connection to a leased or public switched telephone network (PSTN) over which communication can transit?

Does the CS/CDA have a point-to-point (or multi-point) synchronous or asynchronous serial communications link to another computer?

e. Wireless communications with the CDA

Does the CS/CDA have any type of enabled wireless communications adapter (including infrared)?

f. Identification of an attack pathway:

If the CS/CDA is not physically secured in a manner that prevents unauthorized and undetected physical access to the CS/CDA (including its communication connections, local ports, interfaces, the basic input / output system (BIOS) software, and peripheral devices) then the inspector may conclude that physical access to the CS/CDA does provide an attack pathway. (National Institute of Standards and Technology (NIST) SP 800-147)

Some CS/CDAs may incorporate a local HMI that provides some level of user access. In the case of a computer system, the HMI may be a full-graphic cathode ray tube or flat-panel display coupled with a keyboard and mouse. For specialized and less-capable CS/CDAs the HMI could be a simple numeric keypad and multi-line tabular display. The important consideration is whether an attacker could cause adverse impacts to the SSEP functions via this HMI. If so, then the inspector must determine if there are effective physical and/or logical mechanisms in place to prevent access to, and abuse of the HMI by an unauthorized person. If the HMI is physically protected with control over the physical access which prevents unauthorized access, or logically protected (e.g., with multi-factor authentication and strong passwords) which prevents unauthorized access, then the inspector may conclude that physical access to the CS/CDA HMI does NOT provide an attack pathway. If the physical access or physical pathway is only made available to individuals who have been determined to be trustworthy and reliable in accordance with 10 CFR 73.56, and the licensee would be able to detect and respond to unauthorized access, then the vulnerability is diminished and inspector(s) may determine the significance of a finding to be very low provided no adverse impact to an SSEP function has occurred because of a cyberattack (NIST SP 800-123, NIST SP 800-46).

If a licensee has protected CSs/CDAs by effectively implementing the supply chain and services and acquisition protection, in accordance with its CSP, then those CSs/CDAs will be considered as having no attack pathway via the supply chain.

If a CS/CDA is configured to interface with and read-from any form of portable media, then that capability can be used as a pathway for malware delivery. Examples of portable media includes but are not limited to media such as compact disc, digital video disc, Blu-Ray disks, floppy disks, magnetic tape, universal serial bus (USB) “thumb drives,” memory sticks - cards and other such electronic storage devices. If the following controls are effectively implemented, then the inspector may conclude that portable media usage does NOT provide an attack pathway:(1) automatic volume/file-system mounting features are disabled, (2) driver installation using “Plug-N-Play” functionality is disabled, (3) only physically controlled, identifiable, authorized and traceable media is allowed to be connected to the CS/CDA, (4) media is subjected to cleaning such that malware and exploits cannot transit the media, and (5) the licensee has removed and/or

disabled software components that are not required for the operation and maintenance of the CS/CDA (NEI 08-09 and RG 5.71).

If a CS/CDA is configured to interface to, and communicate with, any form of portable computer (intelligent) device, then that connectivity could provide a pathway for delivery of malware.

Portable computer/intelligent devices include obvious devices such as laptop personal computers and personal digital assistants but can also include any such microprocessor-based devices capable of supporting an internal file system such as a “smart” thumb drive (one with encryption and integral security features), an external hard disk drive (connected via USB, FireWire, small computer system interface, Ethernet), an MP3 player, a digital camera or video recorder, a cell phone or even a printer. A large number of devices that use USB or Ethernet connectivity would be included in this broad category. For some Ethernet and USB-connected devices, the CS/CDA operating system may permit those devices to install a ‘driver’ on the CS/CDA via “Plug-N-Play” functions and protocols, which can provide a means for malware delivery. If the following controls are effectively implemented, then the inspector may conclude that portable device usage does not provide an attack pathway: (1) automatic volume/file- system mounting features are disabled; (2) driver installation using “Plug-N-Play” functionality is disabled; (3) only physically controlled, identifiable, authorized and traceable devices are allowed to be connected to the CS/CDA; (4) the licensee has removed and/or disabled software components that are not authorized nor required for the operation and maintenance of the CS/CDA (NEI 08-09).

If a CS/CDA has an enabled network interface and wired communications connection into any form of LAN or WAN, then that communications connectivity may provide an attack pathway. Examples of applicable LAN/WAN technology include any form of Institute of Electrical and Electronics Engineers (IEEE)-802.5 (Ethernet), Asynchronous Transfer Mode, Fiber Distributed Data Interface topology, frame relay, synchronous optical networking (SONET), Token Ring and X.25 networks.

If the network wiring and infrastructure elements (e.g., switches, hubs, repeaters, etc.) are not accessible to unauthorized access, and are under the licensee’s control, and if the network is employing internet protocol security mechanisms, using FIPS 140-2 or later encryption standards on the CS/CDA, and on the intercommunicating computers/devices to provide communication confidentiality, integrity and source authentication, then the inspector may conclude that the network communications connectivity does NOT provide an attack pathway (NIST SP 800-77). (Note: If the intercommunicating computers are not effectively secured, then they could provide a pathway regardless of the security of the network itself.) Likewise, if the CS/CDA has an enabled network interface and wired communications connection into any form of LAN or WAN, but is separated from all other computers/devices on that LAN/WAN by a boundary protective device that meets the requirements of the licensee’s CSP, the inspector may conclude that the network communications connectivity does NOT provide an attack pathway (NEI 08-09 and RG 5.71).

If the CS/CDA has a dedicated point-to-point serial communications link (e.g., standards EIA-232, EIA-422, EIA-485 or USB) including one based on PSTN dial-in/dial-out, or leased analog telephone circuits, that provides a communication connection, then that communications connectivity provides a potential attack pathway. If the communication

wiring and infrastructure elements are not physically controlled and secured by the licensee, then the potential of the link as an attack pathway is even greater. If the point-to-point communications link wiring and infrastructure elements are not accessible to unauthorized access, and are under the licensee's control, and if the point-to-point communications link is employing internet protocol security mechanisms FIPS 140-2 or later encryption standards on the CS/CDA and on the intercommunicating computers/devices to provide communication confidentiality, integrity and source authentication, and the intercommunicating computer/device is physically secured, access is controlled and has equal cybersecurity protections as the CS/CDA, then the inspector may conclude that the point-to-point communications link does not provide an attack pathway (NIST SP 800-77, NISP SP 800-46).

If a CS/CDA has an enabled wireless communications adapter and communications connection in any form, an attack pathway exists. The use of wireless communications is inherently not secure from eavesdropping, interference, or message injection (NIST SP 800-97).

The above overview provides examples of common pathways. Inspector(s) in the course of inspection effort may discover other pathways which would be exploitable.

04.07 Step 2 – Identification of Exploitable Cybersecurity Vulnerabilities

Requirements in the rule and the CSP such as hardening, defense in depth, and many other security measures and controls, if implemented effectively by the licensee, should eliminate exploitable cybersecurity vulnerabilities. If all of the following filter questions are answered in the negative, then the process is complete and the inspector should conclude that the finding is of very low significance. If any produce a "yes" response, then there is an exploitable cybersecurity vulnerability that could be used against a CS/CDA. In that case, the inspector should proceed to the next phase of verification, 04.08 Step 3 – Assessment of Attack Detection and Response Capabilities. The inspector should refer to NEI 08-09 and the guidance at the end of this section for supplementary information about how to determine the proper answer to these questions.

a. Operating System.

Is the CS/CDA running an operating system that has cybersecurity vulnerabilities that would be exploitable?

b. Networking Support.

Are there network/stack cybersecurity vulnerabilities that would be exploitable?

Are there network service cybersecurity vulnerabilities that would be exploitable?

Are there network services running on the CS/CDA that use insecure protocols that would be exploitable?

c. Software Applications.

Is the CS/CDA running any applications that have cybersecurity vulnerabilities that would be exploitable?

d. Web Services.

Is the CS/CDA running a web server or browser version (including add-ons, plug-ins, and extensions) that have cybersecurity vulnerabilities that would be exploitable?

Are applicable web server, web pages and/or web applications susceptible to Cybersecurity vulnerabilities that would be exploitable?

e. Email Services.

Is the CS/CDA running an email server or client version (including add-ons and extensions) that have cybersecurity vulnerabilities that would be exploitable?

Is the Email server or client using insecure protocols that would be exploitable?

f. Relational Database.

Is the CS/CDA running a relational database management system (RDBMS) (including add-ons and extensions) that has cybersecurity vulnerabilities that would be exploitable?

Is the RDBMS accessible to remote clients via insecure protocols and/or insecure authentication mechanisms?

g. Hardening.

Are there vulnerable services running on the CS/CDA or open ports which create Cybersecurity vulnerabilities that would be exploitable?

Are there policy settings on the CS/CDA that allow for cybersecurity vulnerabilities that would be exploitable?

Are there applications or utilities on the CS/CDA that allow for cybersecurity vulnerabilities that would be exploitable?

h. Licensee vulnerability scans.

Has the licensee failed to correct/address any of the security cybersecurity vulnerabilities identified in the most recent security scan and/or assessment that would be exploitable?

Cybersecurity Vulnerability Identification:

“Zero Day” cybersecurity vulnerabilities exist in many cases; however, the specifics of these cybersecurity vulnerabilities are unknown until they are manifested. Commercial operating systems (including diskless and embedded versions) have a long list of ‘fixes’ (security patches and revision updates) for known cybersecurity vulnerabilities (NIST SP 800-51). If a CS/CDA operating system is of any commercial variation and is not currently patched to the most recent level (or updated to the latest release), then it contains known cybersecurity vulnerabilities, some of which may be locally or remotely exploitable as a means for causing the CS/CDA to execute ‘arbitrary code’ as part of a cyberattack. It is important to differentiate between local and remote exploits since their usefulness depends on certain factors, not the least of which is the availability of a suitable attack pathway (remote exploits require a communications channel, whereas local exploits require local delivery and possibly the presence of system tools such as

compilers) DHS Common Cyber Security Vulnerabilities in Industrial Control Systems (2011).

Many commercial industrial automation devices (e.g., programmable logic controllers, analyzers, smart instruments) have transmission control protocol (TCP) / internet protocol software “stacks” that do not support a comprehensive set of error handlers; which means that under certain conditions sending mal-formed messages, over-sized messages, out of sequence messages, etc., can cause the network software of the device to “crash.’’ Generally, this causes a denial of service condition where the device is unable to communicate until reset (NIST SP 800-82).

Any service or application that communicates with external clients using insecure protocols, particularly protocols where user credentials are passed in clear text (text with nothing done to obscure its content) as part of the session initiation, present a cybersecurity vulnerability in that if an attacker is able to “sniff” the communications traffic, then valid user credentials would be disclosed. If an attacker can gain physical access to a common network, then this can occur. Examples of these applications and services are proprietary CS/CDA protocols and remote access services, such as telecommunications network, file transfer protocol, remote shell, remote execution, and remote login, which don’t encrypt the password or obfuscate it with a one-way hash function (Department of Homeland Security (DHS) Common Cyber Security Vulnerabilities in Industrial Control Systems (2011)).

In regard to hardening, some commercial automation systems/devices are running older versions of operating systems which come in a default distribution configuration in which all of the underlying networking functions are enabled. This includes support for the NetBIOS over TCP and server message block application layer protocol that is used for file/disk sharing. It may also mean the “shares” (administrative or user-defined) are enabled and that null sessions are allowed. These protocols and settings provide exploitable cybersecurity vulnerabilities. Decreasing the number of installed applications and services decreases the cybersecurity vulnerabilities on a computer or system (Department of Homeland Security (DHS) Common Cyber Security Vulnerabilities in Industrial Control Systems (2011)).

The above overview provides examples of common Cybersecurity vulnerabilities. Inspector(s) in the course of inspection effort may discover other Cybersecurity vulnerabilities which would be exploitable.

04.08 Step 3 – Assessment of Attack Detection and Response Capabilities

Requirements in the rule and the CSP such as detection, response, hardening, defense in depth, and many other security measures and controls, if implemented effectively by the licensee, should provide for effective detection and response. Absent an actual cyberattack that adversely impacts an SSEP function, if the answer to all the following questions are yes, then the inspector may determine that the licensee has a program that demonstrates detection and response capabilities before the functions identified by 10 CFR 73.54 are adversely impacted due to cyberattacks. If the answer to any of the following questions is in the negative, then the inspector shall perform a detailed assessment of the licensee’s capability to detect and respond before adverse impact.

a. Attack Detection

Did the licensee place its detection capability along the attack pathway at a place where it can timely detect, respond, and ensure that functions identified by 10 CFR 73.54 are not adversely impacted due to cyberattacks?

Are personnel responsible for cyberattack detection, trained in accordance with licensee training standards and sensitive to indications of a cyberattack?

Does the licensee use whitelisting strategies if technically possible?

If signature based detection is a technically possible and used approach to the detection strategy, does the licensee update the signature indicators?

Does the licensee use anomaly indicators as part of its detection strategy and update the anomaly indicators as required?

If an intrusion detection system (IDS) is used, is the IDS capable of detecting unauthorized changes to itself?

b. Response to Attack

Does the licensee have year-round, 24 hours per day, trained incident response support personnel who offer advice and assistance in response, or use an offsite cybersecurity operations center manned by trained (in accordance with licensee training standards) personnel to assess and respond to cyberattack alarm conditions?

Has the licensee developed procedures for response to ensure that the functions identified by 10 CFR 73.54 are not adversely impacted due to cyberattacks?

Are procedures tested?

Is equipment the personnel use for response available to them?

Is the environment the personnel respond in conducive to successful response?

c. Timely Detection and Response

There are three basic technologies employed to detect cyberattacks in real-time: firewalls, host intrusion detection systems, and network intrusion detection systems (NIDS). Depending on the specific type of technology and its implementation, all three of these can detect as well as block or terminate attacks. Although network access control is not specifically an attack detection technology, it can provide logging and alerts of unsuccessful access attempts which may be a detection strategy. There are other technologies that can identify attempted malicious activity, such as a log collection and analysis application, but these tend not to operate in real time and don’t have the ability to block/terminate attacks as they occur. Another means for detecting attacks is to implement a ‘honeypot’ and/or ‘honeynet’ which are usually virtual systems designed to simulate real systems and provide a target of interest to attract the attention of potential attackers and thereby provide a strategy for detection. Since there is no valid reason for communications with them, the detection of such traffic is a strong indication of some form of attack or attempted attack (NIST SP 800-92).

There are also several technologies that can be used for “after the fact” detection of a successful cyberattack: malware scanners (for bulk-storage and memory) that use signature - based detection, IDS that watch for anomalous application behaviors, file checkers that re-compute and compare to pre-calculated hash codes and white/black listing tools that prevent unauthorized applications from executing (NIST SP 800-94). These automated approaches may still require human interaction for assessment and response (DHS Recommended Practice: Developing an Industrial control Systems Cyber Security Incident Response Capability).

The licensee is required to apply and maintain protective strategies that ensure the capability to timely detect, respond to, and recover from cyberattacks. To be effective, the licensee’s strategy should address the types of attacks and the type of response and time needed to protect SSEP functions against each type (NIST SP 800-82). For many organizations, the most challenging part of the attack response process is accurately detecting and assessing possible incidents (NIST SP 800-61). If attack detection relies on the manual review of event logs and alerts, then it is essential that the process involved, and associated manning/staffing levels, do not result in significant time lags between event (attack) detection and attack termination before adverse impact.

The timeframe available for effective detection and response to a cyberattack is dependent upon several factors and can vary from near real-time to extended time intervals (days and even weeks). Depending on the design and functions of self-spreading opportunistic malicious software (malware) such as viruses, worms, and payloads such as rootkits and backdoors, and the environment into which they are injected, the licensee has differing amounts of time in which to detect and respond in order to protect against adverse impacts to the targeted SSEP function (NISP SP-61).

The first major factor is the design function of the malware. If the malware is designed to seek out given system resources, and those are not present, then the malware may sit idle and the response time necessary is longer. If the malware is a self-replicating worm for example, that consumes resources on the target system thus eventually causing it to crash, the response time necessary may be shorter and involve minutes if not seconds. If the malware needs to establish an out-going TCP/internet protocol connection to its originator (e.g., calling home for instructions) and this isn’t possible, then the allowable response timeframe before adverse impact to SSEP functions could be extensive. On the other hand, if an attacker is actively taking control of a critical system via a zero-day exploit and will use that control to disable that system or possibly manipulate that system in a malicious manner, then the time necessary for response may be only seconds.

Environmental considerations are another factor and will also impact the necessary response time needed before adverse impact. Air gapped systems, and those behind a one-way deterministic device, tend to foil malware that is designed to make a network connection across the Internet to one or more internet protocol (IP) addresses. Systems that have been hardened may be missing many of the system resources needed for malware to establish itself and spread. The presence of a suitably sophisticated “honeypot” or “honeynet” may attract an attacker away from the real critical systems providing time for the cyber responder to mitigate before adverse impact.

The application of white-listing technology may prevent malware that manages to get into a system from being able to execute. Internal firewalls and intrusion detection may

mitigate or stop the spread of malware and provide cyber responders time to respond and act. There are multiple controls described in the CSP, that if implemented will make it difficult if not impossible for malware to function. If effectively implemented, these controls provide more response time to cyber responders.

Any technology that uses signatures or rules as a basis for detection requires that these be up to date in order to address the constantly changing and growing list of known malware and attack methodologies. If the licensee isn't maintaining the currency of their signatures and rule sets, then their cyberattack detection capability is degraded. The longer the time elapsed since the last update the greater the potential for there being undetectable attacks and malware.

Some of the technologies that can detect attacks and malware are also able to block them depending on their configuration. A NIDS can be optionally used as an intrusion prevention technology if physically and logically positioned between attack sources and the CS/CDAs so that it has an ability to discard malicious message traffic, block source IP addresses and terminate network sessions (NIST SP 800-94).

Detection of anomalous activity or behavior is another means of detecting a cyberattack. If implemented effectively, this form of detection could detect "zero day" exploits before adverse impact to SSEP functions. Below is a list, which is not all inclusive, of anomalous activity which could be indicative of attack (NEI 08-09 Rev 6 and RG 5.71, DHS Recommended Practice: Developing an Industrial Control Systems Cyber Security Incident Response Capability).

- Unusual and or heavy network traffic
- Out of disk space or significantly reduced free disk space
- Unusually high processing unit or memory usage
- Large numbers of identical running processes
- Unidentified running services or processes
- Unusual protocol behavior
- Unusual application behavior
- Unusual registry changes
- Unusual file changes
- Unusual time of day or day of week activity
- Unusual creation of new user or administrator accounts
- Attempted or actual use of administrator-level accounts
- Locked-out accounts
- Cleared log files
- Unusual information flow exiting the system
- Full log files with unusually large number of events
- Disabled antivirus software and other security controls
- Unexpected patch changes
- Attempted connections to outside IP addresses
- Unexpected changes in configuration settings
- Unexpected system shutdown
- Creation of new address resolution protocol addresses
- Unusual activity from control devices*
- Unusual activity in an industrial control system (ICS) searching for the tag or points database*

- Filenames containing unusual characters or new or unexpected files and directories
- Erratic equipment behavior, especially when more than one device exhibits the same behavior
- Any apparent override of safety, backup, or failover systems equipment, servers
- Network traffic that has bursts of temporary high usage when the operation process itself is steady and predictable
- Unusual file creation, deletion, or modification
- Unusual IDS or anti-virus software behavior
- Unknown or unusual traffic from corporate or other network external to control systems network*
- Unknown or unexpected firmware “pulls” or “pushes”
- Use of unauthorized protocols
- Unusual time of day or day of week activity
- Inability to send commands to control devices*
- Loss of data/indications from measurement and control devices*
- Loss of signal from control devices*

*These anomalies are primarily associated with ICSs

The above overview provides examples of common detection and response methods. Inspector(s) in the course of inspection effort may discover new methods whereby adversaries can avoid detection.

04.09 Step 4 – Assessment of Mitigation Capabilities

Requirements in the rule and the CSP such as detection, response, hardening, defense in depth, and many other security measures and controls, if implemented effectively by the licensee, should provide for effective mitigation. For the following Step 4 filter questions, if any produce a “yes” response, then the licensee would be incapable of mitigating the impacts of a cyberattack on the CS/CDA. In that case, the inspector should proceed to the next phase of determination by using either Figures 3, 4, or 5 (based on the SSEP function at risk) to make the final significance determination. If the following filter questions are answered in the negative, then the process is complete, and the inspector should conclude that the deficiency is of very low significance. The inspector should refer to the guidance at the end of this section for supplementary information about how to determine the proper answer to these questions.

a. Would manual or automated mitigation reaction time to a cyberattack occur too slowly to prevent an adverse impact to an SSEP function?

b. Would manual or automated mitigation be ineffective to prevent an adverse impact to an SSEP function?

Mitigation to prevent adverse impact to SSEP functions:

Response taken as a result of a cyberattack and mitigation actions must occur within the timeframe necessary to prevent adverse impact to any SSEP functions.

Licensees may use automated or manual actions to mitigate cyberattacks before adverse impact to SSEP functions. These mitigation measures must be effective to ensure protection of the SSEP functions.

If the licensee uses operator or manual actions to protect SSEP functions against a cyberattack, these actions must be accomplished to prevent or mitigate adverse impact to SSEP functions. See the guidance in the inspection procedure to determine the effectiveness of these actions.

The above overview provides a discussion of mitigating the impact of cyberattacks. Inspector(s) in the course of inspection effort may discover new methods whereby adversaries can nullify the effectiveness of mitigation efforts.

0609EIV-05 GUIDANCE

05.01 General Guidance

This section provides guidance for inspectors on determining the significance of inspection findings. The following specific guidance statements address common challenges and lessons learned in the field. These insights are designed to help inspectors navigate the nuances of the inspection process effectively and ensure consistent assessments.

05.02 Evaluating Impact to Safety Related/Important-To-Safety-Functions (Figure 3)

If the preceding evaluation steps results in a determination that a condition exists that would result in an adverse impact to a safety related or import-to-safety function, then the inspector(s) will refer to Figure 3 “Safety Related/Important-to-Safety Significance Determination” and follow these associated assessment steps.

If needed, cybersecurity inspector(s) should consider support from Resident Inspectors or Senior Reactor Analysts when making this determination. A more detailed risk significance assessment may be conducted if the assessment using Figure 3 does not accurately represent the finding. The additional assessment may include an estimate of conditional core damage probability or the change in core damage frequency given the plant-specific systems, structures, and components (SSCs) that would be adversely impacted, the exposure time, and other applicable assumptions. In addition, a more detailed assessment should include the basis for any differences between the screening outcome from Figure 3 and the more detailed assessment. This additional assessment shall not be used for issues associated with an initiation of a plant trip (Step 4a).

Step 1a – Potential Loss of Off-Site Power or Loss of emergency Alternating Current Power

If the finding demonstrates that a cyberattack on digital equipment, a computer, communication systems, or networks under NRC regulatory authority, would cause a loss of off-site power (LOOP) or loss of emergency alternating current (AC) power, then the inspector(s) should proceed to Step 1b below to determine the significance of the finding. Otherwise, the inspector(s) should proceed to Step 2a, below.

Multiple SSCs may be impacted (either individually or in combination) that would result in a loss of emergency AC power. The focus should be on whether or not the emergency AC power function would be lost or maintained.

Step 1b – Potential for Station Blackout

If the finding demonstrates that a cyberattack on digital equipment, a computer, communication systems, or networks under NRC regulatory authority would cause a Station Blackout (SBO), then the inspector(s) should proceed to Step 1c below to determine the significance of the finding. Otherwise, the inspector(s) should determine the finding to be of low to moderate significance.

Step 1c – Potential Inability to Perform a Safe Shutdown

If the finding demonstrates a cyberattack would prevent the ability to achieve and maintain stable hot shutdown and then achieve and maintain stable cold shutdown, then the inspector(s) should determine the finding to be of high significance. If not, then the inspector(s) should determine the finding to be of substantial significance.

There might be multiple mitigating SSCs that have the potential to be impacted (either individually or in combination) that would prevent ability to achieve and maintain stable hot and cold shutdown. The focus should be on whether or not the hot and cold shutdown function would be lost or maintained.

Step 2a - Potential Adverse Impact on the Reactor Protection System

If the finding demonstrates that a cyberattack would cause an adverse impact to the function of the Reactor Protection System (RPS), then the inspector(s) should proceed to Step 2b, below, to determine the significance of the finding. Otherwise, the inspector(s) should proceed to Step 3a, below.

Since the RPS is composed of multiple instruments and circuitry, if any of the components in the RPS would be adversely impacted such that a single instrument, channel, relay, breaker, etc., would not be able to perform its intended function, proceed to Step 2b for additional evaluation.

Step 2b - Potential Unavailability of the Reactor Protection System

If the finding demonstrates that a cyberattack would prevent RPS from performing its intended function, then the inspector(s) should proceed to Step 2c below to determine the significance of the finding. Otherwise, the inspector(s) should determine the finding to be of low to moderate significance.

If certain components within the RPS would be adversely impacted but other redundant components in the RPS capable of performing the same function would not be impacted, the RPS would be considered capable of performing its intended function. For example, if one of four overpressure instrument channels would be adversely impacted but the other three would not be impacted (thus, would satisfy applicable success criteria), then the RPS function would be maintained. Conversely, if three of four overpressure instrument channels would be adversely impacted and the overpressure function of the RPS would not meet its success criteria, then the RPS
would be unable to perform its intended function even though other inputs (e.g., temperature) may be functionally capable to initiate a plant trip.

Step 2c - Potential for an Anticipated Transient Without SCRAM

If the finding demonstrates that a cyberattack would cause an anticipated transient without scram (ATWS) as defined in 10 CFR 50.62(b), then the inspector(s) should determine the finding to be of high significance. If not, then the inspector(s) should determine the finding to be of substantial significance.

For the purposes of this SDP, to meet the ATWS criteria two things need to be met. First, a cyberattack would cause a plant transient that would demand the RPS to initiate a plant trip. Second, a cyberattack would prevent the RPS from initiating a plant trip as demanded by the plant transient.

Step 3a - Potential Adverse Impact to a Risk Significant System Function

If the finding demonstrates that a cyberattack would cause an adverse impact to a risk significant system (RSS) function, then the inspector(s) should proceed to Step 3b, below, to determine the significance of the finding. Otherwise, the inspector(s) should proceed to Step 4a, below.

The RSS function, and associated success criteria that need to be met in order to achieve that function, can be defined by, but not limited to, plant probabilistic risk assessment function, final safety analysis report design or safety function, maintenance rule function, or technical specification or technical requirements manual basis function or documentation required by 10 CFR 73.55 (f). If any of the component(s) in an RSS would be adversely impacted such that the RSS would not be available to perform its intended function, proceed to Step 3b for additional evaluation.

Step 3b - Potential Adverse Impact to One Risk Significant System Function

If the finding demonstrates that a cyberattack would cause an adverse impact to only one RSS, then the inspector(s) should determine the finding to be of low to moderate significance. Otherwise, the inspector(s) should proceed to Step 3c, below.

The main focus for this step should be on whether the RSS was available to perform its intended function. If there are other diverse systems (i.e., defense in depth) that can perform the same safety function (e.g., high pressure water injection) and would not be adversely impacted, those systems cannot be credited in lieu of the RSS which would not be available to perform its intended function. The scope of the system function is limited to each individual system. However, if one RSS would be unable to perform its intended function and as a result prevent another RSS (or multiple) RSS to perform their intended functions, all of the RSS should be considered unable to perform their intended function.

Step 3c - Potential Adverse Impact to Two Risk Significant System Functions

If the finding demonstrates that a cyberattack would cause an adverse impact to two RSS, then the inspector(s) should determine the finding to be of substantial significance. Otherwise, the inspector(s) should determine the finding to be of high significance.

As stated in the guidance section in 05.02.3b, if one RSS would be unable to perform its intended function and as a result prevent another RSS (or multiple RSS) to perform their intended functions, all of the RSS should be considered unable to perform their intended

function. For example, if a controller that supported multiple emergency diesel generators was adversely impacted such that the emergency AC function was lost, and as a result, two other RSS would not be capable to perform their intended function due to their dependency on emergency AC power, a total of three RSS would be unable to perform their intended functions.

Step 4a - Initiation of a Plant Trip

If the finding demonstrates that a cyberattack did cause a plant trip, then the inspector(s) should determine the finding to be of low to moderate significance. Otherwise, the inspector(s) should determine the finding to be of very low significance.

There are multiple SSCs that can cause a plant trip. Refer to the utility's SSC scoping per 10 CFR 50.65(b)(2)(iii) for additional information regarding applicable SSCs.

05.03 Evaluating Impact to Security Functions (Figure 4)

If the preceding evaluation steps in 0609EIV-05 result in a determination that a condition exists that would result in an adverse impact to a security function, then the inspector(s) will refer to the "Baseline Security Significance Determination" (IMC 0609 Appendix E, Part I) and follow the associated assessment steps.

05.04 Evaluating Impact to Emergency Preparedness Functions (Figure 5)

If the preceding evaluation steps in 0609EIV-05 result in a determination that an insecure condition exists that did result in an adverse impact to an emergency preparedness (EP) function, then the inspector(s) will refer to Figure 5 "Emergency Preparedness Significance Determination" and follow the associated assessment steps.

0609EIV-06 REFERENCES

Department of Energy – Idaho National Laboratory, Mitigations for Security Vulnerabilities Found in Control System Networks, © ISA, (2006)

Department of Homeland Security (DHS), Common Cyber Security Vulnerabilities in Industrial Control Systems (2011)

DHS, Recommended Practice: Developing an Industrial Control Systems Cyber Security Incident Response Capability (2009)

DHS, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies (2016)

IMC 0308, Attachment 3, Appendix E, "Technical Basis for the Baseline Security Significance Determination Process"

IMC 0609, Appendix B, "Emergency Preparedness Significance Determination Process"

IMC 0609, Attachment 4, "Initial Characterization of Performance Deficiencies"

IMC 0612, Appendix B, "Issue Screening Directions"

National Institute of Standards and Technology (NIST), SP 800-123, Guide to General Server Security

NIST, SP 800-147, BIOS Protection Guidelines for Servers

NIST, SP 800-40, Guide to Enterprise Patch Management Planning: Preventing Maintenance for Technology

NIST, SP 800-41, Guidelines of Firewalls and Firewall Policy

NIST, SP 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your own Device (BYOD) Security

NIST, SP 800-51, Guide to Using Vulnerability Naming Schemes

NIST, SP 800-61, Computer Security Incident Handling Guide

NIST, SP 800-77, Guide to internet protocol security VPNs Note: The 2020 update of 800-77 references FIPS 140-3 as the cryptographic modules standard vs FIPS 140-2

NIST, SP 800-82, Guide to Operational Technology (OT) Security

NIST, SP 800-83, Guide to Malware Incident Prevention and Handling

NIST, SP 800-92, Guide to Computer Security Log Management

NIST, SP 800-94, Guide to Intrusion Detection and Prevention Systems

NIST, SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i

NEI 08-09 Rev. 7, Cyber Security Plan for Nuclear Power Reactors NRC Enforcement Policy

Regulatory Guide (RG) 5.71, Cyber Security Programs for Nuclear Facilities

RG 5.79, Protection of Safeguards Information

END

List of Exhibits:

List of Attachments

Figure 1: Minor vs More-than-Minor Determination

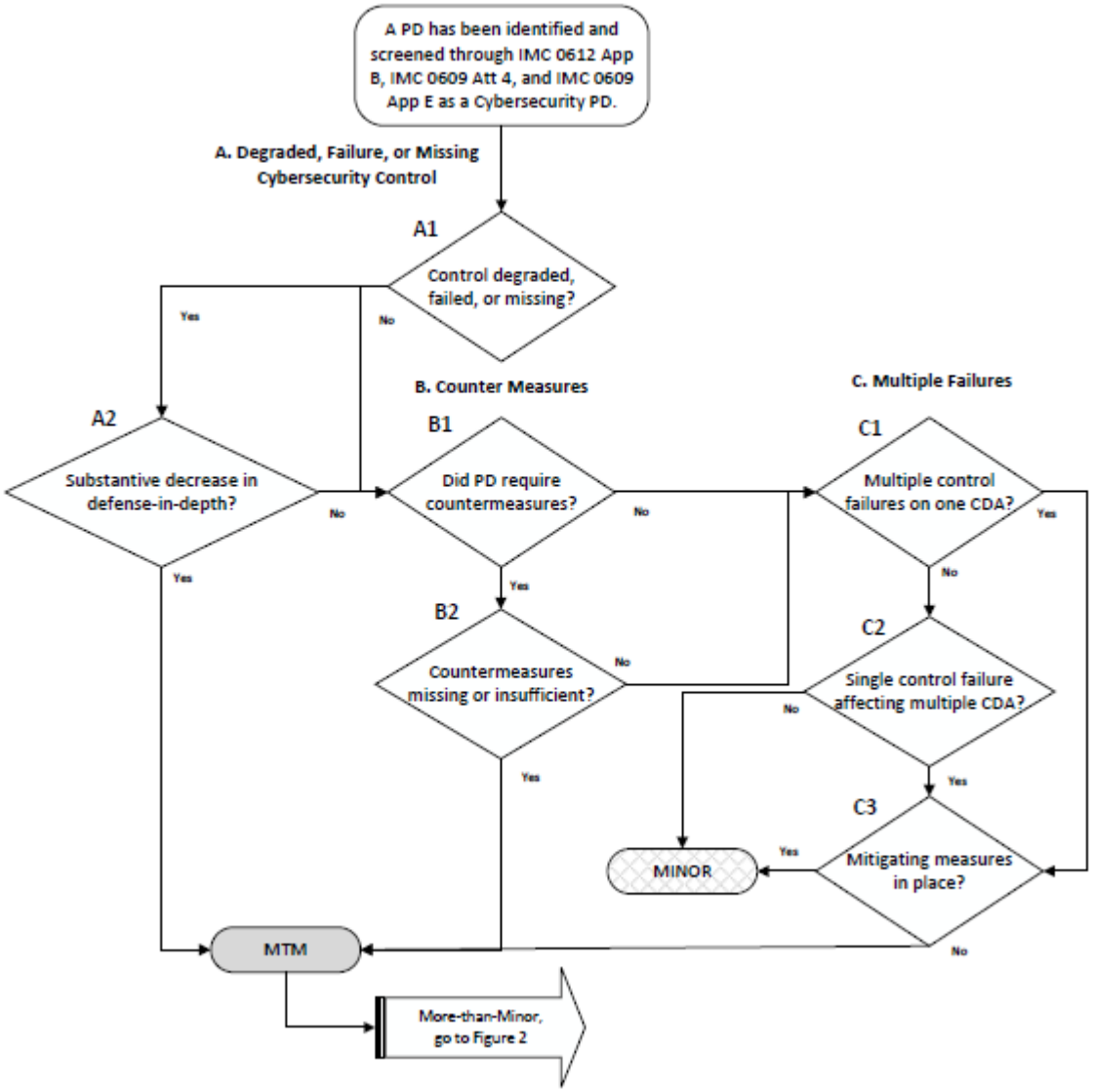


Figure 2: Starting Point for Finding Cybersecurity Significance Determination

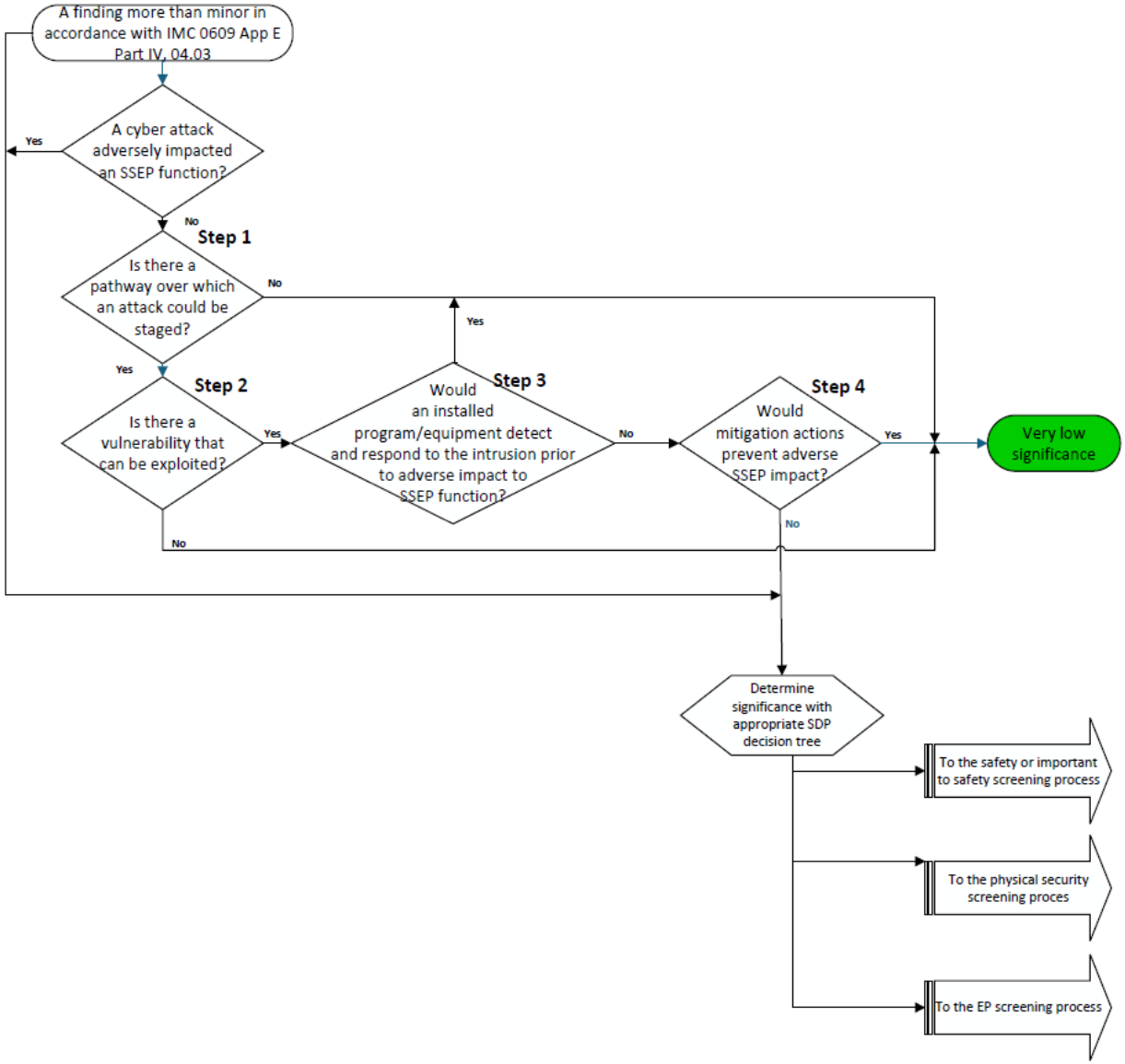


Figure 3: Evaluating Impact to Safety Related/Important-To-Safety Functions

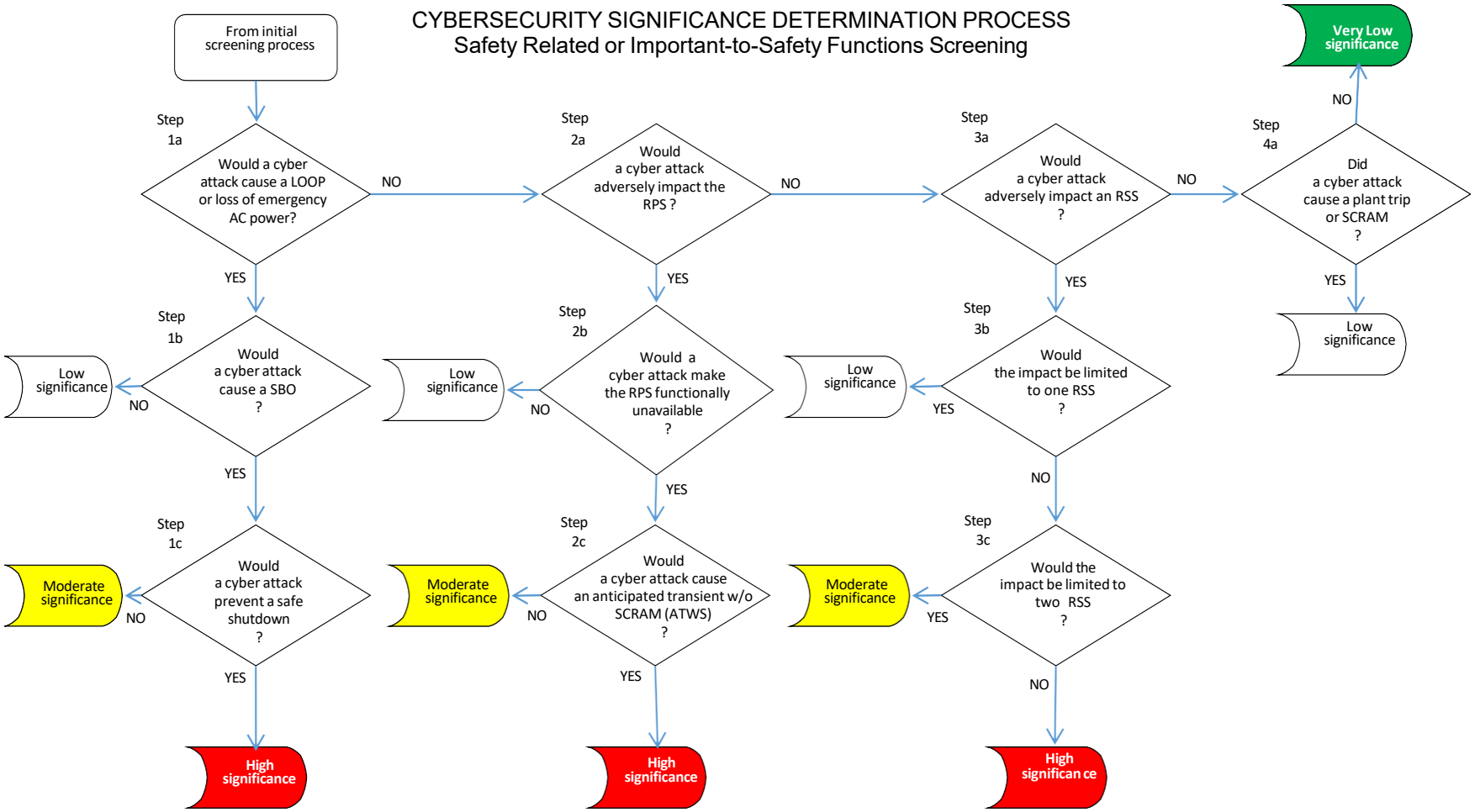


Figure 4: Evaluating Impact to Security Functions

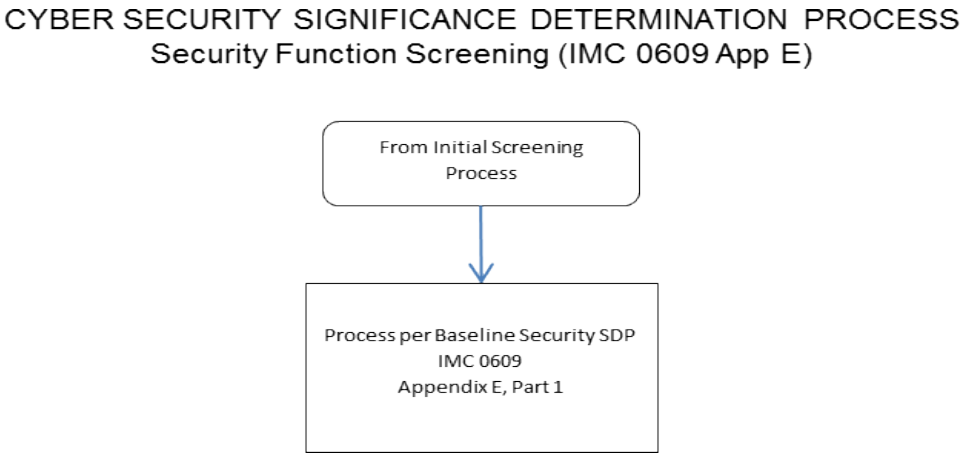
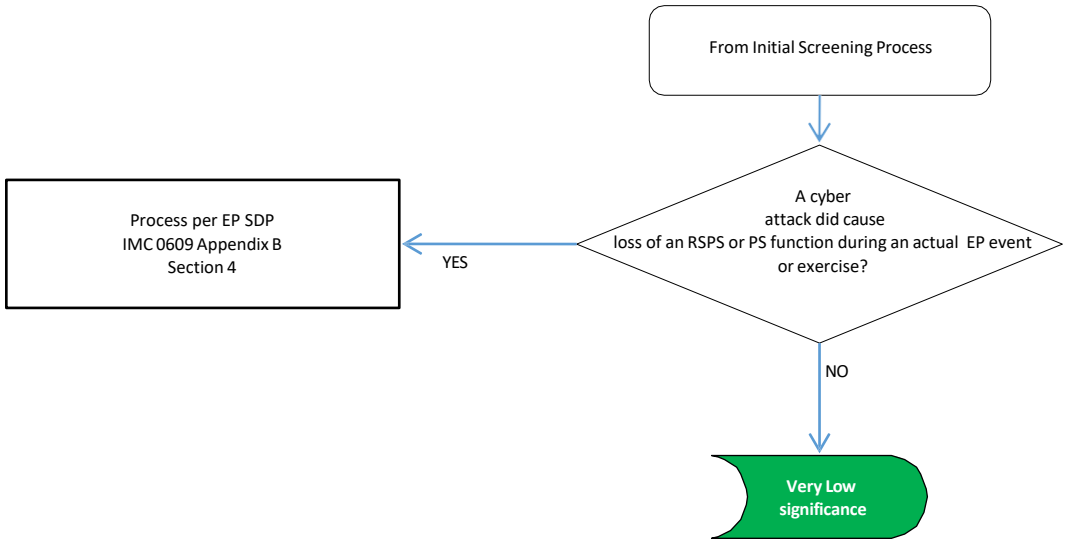


Figure 5: Evaluating Impact to Emergency Preparedness Functions

CYBERSECURITY SIGNIFICANCE DETERMINATION PROCESS
Emergency Preparedness Function Screening (IMC 0609 App B)



Attachment 1: Revision History for IMC 0609, Appendix E, Part IV

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Form Accession Number (Pre-Decisional Non-Public Information)
N/A	ML12318A135 01/24/13 CN 13-003	Initial Issuance. Researched comments in the last 4 years and found none.	N/A	
N/A	ML17115A542 08/15/17 CN 17-014	Revised to reflect lessons learned from interim milestone inspections as well as input received from the Regions and Industry.	N/A	ML17115A543
N/A	ML24257A109 02/19/25 CN 25-003	Revised to reflect current NRC formatting requirements and to remove superseded references. Added portion markers in accordance with RG 5.79. No substantive changes made.	N/A	ML24257A110
N/A	ML25328A204 05/08/26 CN 26-021	This document was revised to incorporate changes to the minor and more than minor screening process. This revision included a determination that this IMC is no longer Official Use Only – Security-Related Information.	N/A	ML25328A207