

1 Discussion Draft of the Preliminary Cybersecurity Framework

2 Illustrative Examples

3 The Cybersecurity Framework emphasizes processes/capabilities and supports a broad range of
4 technical solutions. While organizations and sectors may develop overall Profiles, these Threat
5 Mitigation Profile examples that illustrate how organizations may apply the Framework to
6 mitigate specific threats. These scenarios include cybersecurity intrusion, malware, and insider
7 threat.

8

9 Threat Mitigation Examples

10 A threat is characterized as any circumstance or event with the potential to have an adverse
11 impact on an information system through unauthorized access, destruction, disclosure,
12 modification of data, and/or denial of service (DoS). Threats continue to evolve in sophistication,
13 moving from exploitation (collection and interception of information) to disruption (denial of
14 service attacks) to destruction, with physical damage to a main operating component, whether it
15 is destruction of information or incorrect commands causing damage to computer-controlled
16 systems. The following examples describe Profiles crafted to address specific known threats.

17 Example 1: Mitigating Cybersecurity Intrusions

18 This example Profile is intended to describe key activities that address the cybersecurity risk
19 associated with a Cybersecurity Intrusion event. The Profile was crafted based on the activities
20 performed by adversaries during the life cycle of a cybersecurity intrusion. The cybersecurity
21 intrusion life cycle consists of three general phases: Gain Access, Maintain Access, and Act.

22 **Gain Access:** The goal of this phase is to achieve limited access to a device on a target
23 network. Adversaries often gain initial access to networks by exploiting a single
24 vulnerability in a product or by prompting user action. Techniques used include: spear
25 phishing, malicious e-mail content, Web browser attacks, exploitation of well-known
26 software flaws, and distribution of malware on removable media.

27 **Maintain Access:** During this phase the adversary takes steps to ensure continued access
28 to the targeted network. This is often accomplished by the installation of tools and/or
29 malware to allow the adversary to maintain a presence on the network. Malware
30 components establish command and control capabilities for the adversary and enable
31 additional attacks to be performed, such as capturing keystrokes and credentials. Example
32 actions taken during this phase include the installation of rootkits/backdoor programs and
33 execution of BIOS exploits.

34 **Act:** In the final phase the adversary focuses on gaining access privileges that enable
35 them to move, compromise, disrupt, exploit, or destroy data. Using the previously
36 established command and control capabilities and compromised accounts, adversaries
37 take steps to access and control additional data and resources. This includes establishing
38 communications channels to the adversary's servers that facilitate remote access.
39 Privilege escalation and lateral movement enable an enterprise-wide compromise by an
40 adversary. The adversary is able to use the access gained to internal networks, where
41 security protections may not be as robust, to gain access to critical resources.

42

Threat Mitigation Profile: Cybersecurity Intrusion

Function	Category	Subcategories	IR	Comment
Identify	Risk Assessment	<ul style="list-style-type: none"> Identify threats to organizational assets (both internal and external) Identify providers of threat information 	<p>NIST SP 800-53 Rev. 4 PM-16</p> <p>ISO/IEC 27001 A.13.1.2</p>	Allows the organization to identify current known IP addresses for adversary servers and block inbound and outbound connections to this source.
Protect	Awareness and Training	<ul style="list-style-type: none"> Provide awareness and training that ensures that general users understand roles & responsibilities and act accordingly Provide awareness and training that ensures that privileged users (e.g. system, network, industrial control system, database administrators) understand roles & responsibilities and act accordingly Provide awareness and training that ensures that third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities and act accordingly Provide awareness and training that ensures that senior executives understand roles & responsibilities and act accordingly Provide awareness and training that ensures that physical and information security personnel understand roles & responsibilities and act accordingly 	CCS CSC9	Training that is shaped by the existing threat landscape provides employees with an awareness of active threats and the basic cybersecurity knowledge needed to identify suspicious applications and not to open unknown email attachments. The benefit of awareness and training can be extremely high and has a relatively low cost.
Protect	Information Protection Processes and Procedures	<ul style="list-style-type: none"> Develop, document, and maintain under configuration control a current baseline configuration of information technology / operations technology systems 	<p>NIST SP 800-53 Rev. 4 CM-2</p>	An effective patch management process provides another potential defense against malware. Many exploits use well-known software flaws for which patches are available. A mature patch management process makes it harder

Function	Category	Subcategories	IR	Comment
				for an adversary to craft an initial exploit. It is important that critical infrastructure install updated patches; test patches for potential operational impacts; and ensure that the patches do not introduce new vulnerabilities.
Protect	Protective Technology	<ul style="list-style-type: none"> Implement and maintain technology that enforces policies to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on organizational systems (i.e., Whitelisting of applications and network traffic) Determine, document, and implement physical and logical system audit and log records in accordance with organizational auditing policy 	<p>CCS CSC 6</p> <p>COBIT APO11.04</p>	<p>Application whitelisting ensures that only approved applications may run. This mitigation approach can also prevent the installation of known malicious code.</p> <p>Auditing and logging operates in direct support of other Detect, Respond, and Recover Framework Functions.</p>
Detect	Security Continuous Monitoring	<ul style="list-style-type: none"> Perform network monitoring for cybersecurity events flagged by the detection system or process Perform physical monitoring for cybersecurity events flagged by the detection system or process Perform personnel monitoring for cybersecurity events flagged by the detection system or process Employ malicious code detection mechanisms on network devices and systems to detect and eradicate malicious code Detect the use of mobile code and implement corrective actions when unacceptable mobile code is detected Perform personnel and system monitoring activities over external service providers 	<p>NIST SP 800-53 Rev. 4 CM-1, CA-7, AC-2, SC-5, SI-4</p> <p>NIST SP 800-53 Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20</p> <p>NIST SP 800-53 Rev. 4 CM-1, CA-7</p> <p>ISO/IEC 27001 A.10.4.2</p> <p>ISO/IEC 27001 10.2.2</p> <p>NIST SP 800-53 Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20</p>	<p>Monitoring can detect and quarantine email that contains malware prior to delivery. Malware can be identified using signatures that uniquely identify specific malware components. Malware signatures must be frequently updated to ensure that emerging malware threats can be identified and eradicated before users within the organization can launch them.</p> <p>Monitoring also allows the organization to detect unusual or anomalous system behaviors that may indicate that a system has been infected with malware. Automated malware detection solutions can be configured to block connections to servers that are known to host malware or that malware</p>

Function	Category	Subcategories	IR	Comment
		<ul style="list-style-type: none"> Perform periodic checks for unauthorized personnel, network connections, devices, software Perform periodic assessments to identify vulnerabilities that could be exploited by adversaries (aka Penetration testing) 	NIST SP 800-53 Rev. 4 CM-1, CA-7	software is known to communicate with.
Respond	Planning	<ul style="list-style-type: none"> Execute the organization's incident response plan 	CCS CSC 18 NIST SP 800-53 Rev. 4 IR-1, IR-2	After an attack is recognized, the security team should use the organization's response plan to determine the appropriate, coordinated response to the type of attack.
Respond	Analysis	<ul style="list-style-type: none"> Investigate anomalies, including cybersecurity events (from network, physical, or personnel monitoring) flagged by the detection system or process Conduct an impact assessment (damage/scope) Perform forensics Classify the incident 	ISO/IEC 27001 A.06.02.01 ISO/IEC 27001 A.06.02.01 ISO/IEC 27001 A.13.02.02 A.13.02.03 ISO/IEC 27001 A.13.0 A.13.02 A.03.06 A.07.4.2.1	It is important to understand the scope of the incident, the extent of damage, the level of sophistication demonstrated by the adversary, and the stage the attack is in. This knowledge helps to determine if an attack is localized on an organization's machine or if the adversary has a persistent presence on the network and the scope is enterprise-wide. Organization should compare attack data against current and predicted attack models to gain meaningful insight into the attack.
Respond	Improvements	<ul style="list-style-type: none"> Incorporate lessons learned into plans Update response strategies 	ISO/IEC 27001 A.13.02.02 NIST SP 800-53 Rev. 4 PM-9	Document the lessons learned from the intrusion and use them to enhance organizational cybersecurity processes.

47 **Example 2: Malware**

48 It has been shown that critical infrastructure can be susceptible to low-level threats that cause
 49 ancillary disruption. Recent attacks suggest that malware infections pose a significant threat to
 50 organizational assets. Key features of malware attacks include the exploitation of outdated
 51 patches, ingress through back channels, denial of service based on exploited systems and failing
 52 network hardware, escalation of presence, and the prevalence of a ‘fortress mentality.’

53
 54 **Threat Mitigation Profile: Malware**

Function	Category	Subcategories	IR	Comment
Identify	Asset Management	<ul style="list-style-type: none"> Inventory and track physical devices and systems within the organization Inventory software platforms and applications within the organization Identify organizational network components and connections Identify external information systems including processing, storage, and service location Identify classification/criticality/business value of hardware, devices, and software 	<p>ISO/IEC 27001 A.7.1.1, A.7.1.2</p> <p>COBIT BAI03.04, BAI09.01, BAI09, BAI09.05</p> <p>ISO/IEC 27001 A.7.1.1</p> <p>NIST SP 500-291 3, 4</p>	Understanding of the network architecture must update with changes. Potential backdoors must be identified and mitigated.
Protect	Access Control	<ul style="list-style-type: none"> Perform identity and credential management (including account management, separation of duties, etc.) for devices and users Enforce physical access control for buildings, stations, substations, data centers, and other locations that house logical and virtual information technology and operations technology Protect remote access to organizational networks to include telework guidance, mobile devices access restrictions, and cloud computing policies/procedures 	<p>NIST SP 800-53 Rev. 4 AC Family</p> <p>ISO/IEC 27001 A.9.1, A.9.2, A.11.4, A.11.6,</p> <p>COBIT APO13.01, DSS01.04, DSS05.03</p>	Access control should be risk informed, should be updated, and should anticipate threats.

Function	Category	Subcategories	IR	Comment
		<ul style="list-style-type: none"> Enforce access restrictions including implementation of Attribute-/Role-based access control, permission revocation, network access control technology Protect network integrity by segregating networks/implementing enclaves 	<p>CCS CSC 12, 15</p> <p>ISO/IEC 27001 A.10.1.4, A.11.4.5</p>	
Protect	Awareness and Training	<ul style="list-style-type: none"> Provide awareness and training that ensures that general users understand roles & responsibilities and act accordingly Provide awareness and training that ensures that privileged users (e.g. system, network, industrial control system, database administrators) understand roles & responsibilities and act accordingly Provide awareness and training that ensures that third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities and act accordingly Provide awareness and training that ensures that senior executives understand roles & responsibilities and act accordingly Provide awareness and training that ensures that physical and information security personnel understand roles & responsibilities and act accordingly 	<p>COBIT APO07.03, BAI05.07</p> <p>ISO/IEC 27001 A.8.2.2</p> <p>NIST SP 800-53 Rev. 4 AT-3</p> <p>CCS CSC 9</p> <p>ISO/IEC 27001 A.8.2.2</p>	<p>Partners must be educated as to the impact they or their systems may have on critical infrastructure.</p> <p>Employees must have ongoing understanding of malware that reflects the current threat landscape.</p>
Protect	Information Protection Processes and Procedures	<ul style="list-style-type: none"> Develop, document, and maintain under configuration control a current baseline configuration of information technology / operations technology systems 	<p>CCS CSC 3, 10</p>	<p>Aggressive patch management is particularly important in the critical infrastructure setting. Patches should be thoroughly tested prior to deployment to ensure that the patch does not negatively</p>

Function	Category	Subcategories	IR	Comment
				affect critical systems. Rapid testing and installation of new patches is critical to hardening the network from malicious code should it penetrate existing barriers.
Protect	Protective Technology	<ul style="list-style-type: none"> Implement and maintain technology that enforces policies to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on organizational systems (i.e., Whitelisting of applications and network traffic) Restrict the use of removable media (including writable portable storage devices), personally/externally owned devices, and network accessible media locations Determine, document, and implement physical and logical system audit and log records in accordance with organizational auditing policy Protect wireless network security including monitoring for unauthorized devices/networks, processes for authorization and authentication for wireless networks, adequate encryption to protect information transmitted wirelessly Protect operational technology (to include ICS, SCADA, DCS) 	<p>CCS CSC 6</p> <p>NIST SP 800-53 Rev. 4 AC-19</p> <p>CCS CSC 14</p> <p>ISO/IEC 27001 10.10.2</p> <p>COBIT APO13.01, BAI03.02</p>	Protection of operational technology is critically important. These devices should be separated from all non-necessary devices. Architecture and security measures must be updated with changes to the network and the cybersecurity landscape.
Detect	Anomalies and Events	<ul style="list-style-type: none"> Identify and determine normal organizational behaviors and expected data flow of personnel, operations technology, and information systems 	<p>NIST SP 800-53 Rev. 4 SI-4 AT-3 CM-2</p>	The organization should have solid understanding of the events that occur on their operational networks.

Function	Category	Subcategories	IR	Comment
		<ul style="list-style-type: none"> Characterize detected events (including through the use of traffic analysis) to understand attack targets and how a detected event is taking place Perform data correlation among to improve detection and awareness by bringing together information from different information sources or sensors. Assess the impact of detected cybersecurity events to inform response & recovery activity 	<p>NIST SP 800-53 Rev. 4 SI-4</p> <p>NIST SP 800-53 Rev. 4 SI-4</p> <p>NIST SP 800-53 Rev. 4 SI-4</p>	
Detect	Security Continuous Monitoring	<ul style="list-style-type: none"> Perform network monitoring for cybersecurity events flagged by the detection system or process Perform physical monitoring for cybersecurity events flagged by the detection system or process Perform personnel monitoring for cybersecurity events flagged by the detection system or process Employ malicious code detection mechanisms on network devices and systems to detect and eradicate malicious code Detect the use of mobile code and implement corrective actions when unacceptable mobile code is detected Perform personnel and system monitoring activities over external service providers Perform periodic checks for unauthorized personnel, network connections, devices, software 	<p>ISO/IEC 27001 A.10.10.2, A.10.10.4 A.10.10.5</p> <p>NIST SP 800-53 Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20</p> <p>NIST SP 800-53 Rev. 4 CM-1, CA-7</p> <p>COBIT DSS05.01</p> <p>ISO/IEC 27001 A.10.4.2</p> <p>ISO/IEC 27001 10.2.2</p> <p>NIST SP 800-53 Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20</p>	<p>Monitoring should be adjusted to detect not only presently understood threats but also predicted threats. Organizations should test systems for vulnerabilities that may expose them to current or predicted threats.</p>

Function	Category	Subcategories	IR	Comment
		<ul style="list-style-type: none"> Perform periodic assessments to identify vulnerabilities that could be exploited by adversaries (aka Penetration testing) 	NIST SP 800-53 Rev. 4 CM-1, CA-7	
Respond	Mitigation	<ul style="list-style-type: none"> Contain the incident Eradicate the incident (includes strengthening controls to prevent incident recurrence) 	ISO/IEC 27001 A.03.06 A.13.02.03	It is crucial that incidents be contained and eradicated. Organizations should be prepared for both existing threats and anticipated threats.
Recover	Recovery Planning	<ul style="list-style-type: none"> Execute recover plan 	ISO/IEC 27001 A.14.1.3 A.14.1.4 A.14.1.5	Organizations should have viable recovery options for both currently understood threats and predicted threats.

56 **Example 3: Mitigating Insider Threats**

57 Insider threats present a significant danger to organizations. In many cases personnel may act as
 58 a conduit for a cybersecurity attack. This may occur through the inadvertent installation of
 59 malware, installation of unauthorized software, the loss of organizational assets, accidental data
 60 exposure or loss, and other unintentional actions. Occasionally, organizational insiders may
 61 actively seek to subvert an organization through corporate espionage or corporate sabotage. In
 62 these cases an insider may pose a significant threat, particularly within critical infrastructure.

63 **Threat Mitigation Profile: Insider Threat**

Function	Category	Subcategories	IR	Comment
Identify	Asset Management	<ul style="list-style-type: none"> Identify business value of workforce functions by role 	<p>NIST SP 800-53 Rev. 4 PM-11</p>	Organizations should have understanding of current workforce, their positions, and the assets to which they have access.
Identify	Governance	<ul style="list-style-type: none"> Identify organizational information security policy Identify information security roles & responsibility, coordination Identify legal/regulatory requirements 	<p>COBIT APO01.03, EA01.01</p> <p>ISO/IEC 27001 A.15.1.1</p>	Organizations should have understanding of policies, procedures, and requirements employees must adhere to. Organizations should understand the lines of communication employees currently use and may use in the future, to include social media, email, and mobile networks.
Protect	Access Control	<ul style="list-style-type: none"> Perform identity and credential management (including account management, separation of duties, etc.) for devices and users Enforce physical access control for buildings, stations, substations, data centers, and other locations that house logical and virtual information technology and operations technology Protect remote access to organizational networks to include telework guidance, mobile devices access restrictions, and cloud computing policies/procedures 	<p>NIST SP 800-53 Rev. 4 AC Family</p> <p>COBIT DSS01.04, DSS05.05</p> <p>ISO/IEC 27001 A.11.4, A.11.7</p>	Organizations should monitor and maintain constant control of credentials, access to facilities and assets, as well as remote access to assets. Furthermore, organizations should continue to search for and mitigate the damage caused by unknown possible points of entry.

Function	Category	Subcategories	IR	Comment
		<ul style="list-style-type: none"> Enforce access restrictions including implementation of Attribute-/Role-based access control, permission revocation, network access control technology Protect network integrity by segregating networks/implementing enclaves 	<p>ISO/IEC 27001 A.11.1.1</p> <p>ISO/IEC 27001 A.10.1.4, A.11.4.5</p>	
Protect	Awareness and Training	<ul style="list-style-type: none"> Provide awareness and training that ensures that general users understand roles & responsibilities and act accordingly Provide awareness and training that ensures that privileged users (e.g. system, network, industrial control system, database administrators) understand roles & responsibilities and act accordingly Provide awareness and training that ensures that third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities and act accordingly Provide awareness and training that ensures that senior executives understand roles & responsibilities and act accordingly Provide awareness and training that ensures that physical and information security personnel understand roles & responsibilities and act accordingly 	<p>COBIT APO07.03, BAI05.07</p> <p>ISO/IEC 27001 A.8.2.2</p> <p>NIST SP 800-53 Rev. 4 AT-3</p> <p>CCS CSC 9</p> <p>ISO/IEC 27001 A.8.2.2</p>	Organizations should have ongoing security training that mirrors current and potential threats. Employees should be trained to identify misuse of assets.
Protect	Data Security	<ul style="list-style-type: none"> Protect data (including physical records) during storage (aka "data at rest") to achieve confidentiality, integrity, and availability goals Protect data (including physical records) during transportation/transmission (aka "data in 	<p>ISO/IEC 27001 A.15.1.3, A.15.1.4</p> <p>NIST SP 800-53 Rev. 4 SC-8</p>	Organizations should seek to protect organizational data at rest from both outside threats and inside threats in a manner that reflects current understanding of the value of the information.

Function	Category	Subcategories	IR	Comment
		<p>motion") to achieve confidentiality, integrity, and availability goals</p> <ul style="list-style-type: none"> <li data-bbox="503 359 917 510">• Protect organizational property and information through the formal management of asset removal, transfers, and disposition <li data-bbox="503 541 917 726">• Protect availability of organizational facilities and systems by ensuring adequate capacity availability (physical space, logical storage/memory capacity) <li data-bbox="503 758 917 999">• Protect confidentiality and integrity of organizational information and records by preventing intentional or unintentional release of information to an unauthorized and/or untrusted environment (information/data leakage) <li data-bbox="503 1031 917 1125">• Protect intellectual property in accordance with organizational requirements <li data-bbox="503 1157 917 1308">• Reduce potential for abuse of authorized privileges by eliminating unnecessary assets, separation of duties procedures, and least privilege requirements <li data-bbox="503 1339 917 1560">• Establish separate development, testing, and operational environments to protect systems from unplanned/unexpected events related to development and testing activities <li data-bbox="503 1591 917 1797">• Protect the privacy of individuals and personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by organizational programs and systems 	<p>ISO/IEC 27001 A.9.2.7</p> <p>ISO/IEC 27001 A.10.3.1</p> <p>CCS CSC 17</p> <p>ISO/IEC 27001 A.15.1.2</p> <p>NIST SP 800-53 Rev. 4 AC-5, AC-6</p> <p>COBIT BAI07.04</p> <p>ISO/IEC 27001 A.15.1.3</p>	

Function	Category	Subcategories	IR	Comment
Protect	Information Protection Processes and Procedures	<ul style="list-style-type: none"> Develop, document, and maintain under configuration control a current baseline configuration of information technology / operations technology systems Develop, document, and maintain a System Development Life Cycle (including secure software development and system engineering and outsourced software development requirements) Protect organizational information by conducting backups that ensure appropriate confidentiality, integrity, and availability of backup information, storing the backed-up information properly, and testing periodically to ensure recoverability of the information Ensure appropriate environmental requirements are met for personnel and technology Destroy/dispose of assets (to include data destruction) in a manner that prevents disclosure of information to unauthorized entities Achieve continued improvement (lessons learned, best practices, feedback, etc.) Develop, document, and communicate response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s) that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance 	<p>NIST SP 800-53 Rev. 4 CM-2</p> <p>CCS CSC 6</p> <p>NIST SP 800-53 Rev. 4 CP-9</p> <p>COBIT DSS01.04, DSS05.05</p> <p>ISO/IEC 27001 9.2.6</p> <p>COBIT APO11.06, DSS04.05</p> <p>ISO/IEC 27001 A.14.1</p>	Organizations should have well-established processes that address the potential damage to operations and business that an insider threat may cause. Processes must also exist to protect data from insiders such as limiting attack surfaces and properly disposing of assets. Processes should also integrate with human resources to ensure that employees are properly screened and adhere to organizational security requirements.

Function	Category	Subcategories	IR	Comment
		<ul style="list-style-type: none"> Plan for what it takes to deliver critical infrastructure services for which the organization is responsible, including the identification of dependencies that might prevent delivery of those services Integrate cybersecurity practices / procedures with human resources management (personnel screenings, departures, transfers, etc.) 	<p>ISO/IEC 27001 9.2.2</p> <p>COBIT APO07.01, APO07.02, APO07.03, APO07.04, APO07.05,</p>	
Protect	Protective Technology	<ul style="list-style-type: none"> Implement and maintain technology that enforces policies to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on organizational systems (i.e., Whitelisting of applications and network traffic) Restrict the use of removable media (including writable portable storage devices), personally/externally owned devices, and network accessible media locations Determine, document, and implement physical and logical system audit and log records in accordance with organizational auditing policy Protect wireless network security including monitoring for unauthorized devices/networks, processes for authorization and authentication for wireless networks, adequate encryption to protect information transmitted wirelessly Protect operational technology (to include ICS, SCADA, DCS) 	<p>CCS CSC 6</p> <p>NIST SP 800-53 Rev. 4 AC-19</p> <p>CCS CSC 14</p> <p>ISO/IEC 27001 10.10.2</p> <p>COBIT APO13.01, BAI03.02</p>	Organizations should ensure continuous security of applications, networks, and devices from insider threats.

Function	Category	Subcategories	IR	Comment
Detect	Anomalies and Events	<p>Identify and determine normal organizational behaviors and expected data flow of personnel, operations technology, and information systems</p> <ul style="list-style-type: none"> Characterize detected events (including through the use of traffic analysis) to understand attack targets and how a detected event is taking place Perform data correlation among to improve detection and awareness by bringing together information from different information sources or sensors. Assess the impact of detected cybersecurity events to inform response & recovery activity 	<p>NIST SP 800-53 Rev. 4 SI-4 AT-3 CM-2</p> <p>NIST SP 800-53 Rev. 4 SI-4</p> <p>NIST SP 800-53 Rev. 4 SI-4</p> <p>NIST SP 800-53 Rev. 4 SI-4</p>	Organizations should assess anomalies within the organizational network.
Detect	Security Continuous Monitoring	<ul style="list-style-type: none"> Perform network monitoring for cybersecurity events flagged by the detection system or process Perform physical monitoring for cybersecurity events flagged by the detection system or process Perform personnel monitoring for cybersecurity events flagged by the detection system or process Employ malicious code detection mechanisms on network devices and systems to detect and eradicate malicious code Detect the use of mobile code and implement corrective actions when unacceptable mobile code is detected Perform personnel and system monitoring activities over external service providers 	<p>ISO/IEC 27001 A.10.10.2, A.10.10.4, A.10.10.5</p> <p>NIST SP 800-53 Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20</p> <p>NIST SP 800-53 Rev. 4 CM-1, CA-7</p> <p>COBIT DSS05.01</p> <p>ISO/IEC 27001 A.10.4.2</p> <p>ISO/IEC 27001 10.2.2</p>	Organizations should have ongoing monitoring of assets to include employee interactions with assets.

Function	Category	Subcategories	IR	Comment
		<ul style="list-style-type: none"> Perform periodic checks for unauthorized personnel, network connections, devices, software Perform periodic assessments to identify vulnerabilities that could be exploited by adversaries (aka Penetration testing) 	<p>NIST SP 800-53 Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20</p> <p>NIST SP 800-53 Rev. 4 CM-1, CA-7</p>	
Detect	Detection Processes	<ul style="list-style-type: none"> Ensure accountability by establishing organizational roles, responsibilities for event detection and response Perform policy compliance and enforcement for detect activities (internal, external constraints) Conduct exercises (e.g., tabletop exercises) to ensure that staff understand roles/responsibilities and to help provide quality assurance of planned processes Communicate and coordinate cybersecurity event information among appropriate parties 	<p>ISO/IEC 27001 A.10.4.2</p> <p>ISO/IEC 27001 A.10.2.2</p> <p>NIST SP 800-53 Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20</p>	Organizations should establish roles, responsibilities, and privileges for employees. They should also ensure employees adhere to organizational policies. Organizations should conduct testing to ensure employees are adhering to policies and procedures, and that new methods of accessing and communicating organizational data are found and controlled.
Respond	Analyze	<ul style="list-style-type: none"> Conduct an impact assessment (damage/scope) Perform forensics Classify the incident 	<p>ISO/IEC 27001 A.06.02.01</p> <p>ISO/IEC 27001 A.13.02.02 A.13.02.03</p> <p>ISO/IEC 27001 A.13.0 A.13.02 A.03.06 A.07.4.2.1</p>	Organizations should conduct a thorough analysis to better understand the impact of insider threat incidents, to help prepare for recovery efforts, and to craft an effective containment and eradication strategy.
Respond	Mitigation	<ul style="list-style-type: none"> Contain the incident Eradicate the incident (includes strengthening controls to prevent incident recurrence) 	<p>ISO/IEC 27001 A.03.06 A.13.02.03</p>	Organizations should implement the steps necessary to manage the insider threat incident and engage law enforcement, as needed, to ensure that the threat is contained and eradicated.
Respond	Improvements	<ul style="list-style-type: none"> Incorporate lessons learned into plans 	<p>ISO/IEC 27001 A.13.02.02</p>	Organizations should document the lessons learned from insider

Function	Category	Subcategories	IR	Comment
		<ul style="list-style-type: none"> Update response strategies 	NIST SP 800-53 Rev. 4 PM-9	threat incidents and incorporate them into response plans and strategy.
Recover	Recovery Planning	<ul style="list-style-type: none"> Execute recover plan 	CCS CSC 8	Organizations should have recovery plans that account for current and predicted insider threats.