AGENDA PACKET

CITY COUNCIL'S COMMITTEE ON GOVERNMENT OPERATIONS, PUBLIC SAFETY
MONDAY, SEPTEMBER 11, 2023 6:00 PM

EVERETT CITY HALL, 484 BROADWAY, CITY COUNCIL CHAMBERS, 3RD FLOOR
EVERETT, MA 02149

AGENDA

CITY COUNCIL'S COMMITTEE ON GOVERNMENT OPERATIONS, PUBLIC SAFETY
MONDAY, SEPTEMBER 11, 2023 6:00 PM

EVERETT CITY HALL, 484 BROADWAY, CITY COUNCIL CHAMBERS, 3RD FLOOR
EVERETT, MA 02149

ROLL CALL

PLEDGE OF ALLEGIANCE

UNFINISHED BUSINESS

1. **C0111-23** Resolution/s/ Councilor Darren M. Costa

   A resolution requesting that the IT Director appear to comment on whether the City of Everett would benefit from appropriating ARPA funding to modernize Cybersecurity, Public-facing Digital Services and Cross-Government Collaboration / Scalable Services. The goal would be to ensure the city is protected from potential cyberattacks and/or data breaches.

ADJOURNMENT

www.cityofeverett.com
(All agendas and reports can be obtained on City of Everett Website)

Respectfully submitted:

Michael J. Mangan

Legislative Aide
Everett City Council Office

City of Everett Massachusetts

C0111-23

To: **Mayor and City Council**

From: **Councilor Darren M. Costa**

Date: March 27, 2023

Agenda Item:
That the Director of Information Technology appear at the next regular meeting of the City Council to discuss the city's cyber security and also to consider using ARPA funding to address any issues

Background and Explanation:

Attachments:

ACCOUNT SECURITY (1.0)

1.1 Detection of Unsuccessful (Automated) Login Attempts PR.AC-7	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Brute Force - Password Guessing (T1110.001) Brute Force - Password Cracking (T1110.002) Brute Force - Password Spraying (T1110.003) Brute Force - Credential Stuffing (T1110.004) **RECOMMENDED ACTION:** All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., 5 failed attempts over 2 minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis. For IT assets, there is a system-enforced policy that prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10 minutes after 10 incorrect logins over a 10 minute period.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

1.2 Changing Default Passwords PR.AC-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Valid Accounts - Default Accounts (T1078.001) Valid Accounts (ICS T0859) **RECOMMENDED ACTION:** An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before being put on any internal or external network. This includes IT assets for OT, such as OT administration web pages. In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices. **OT:** While changing default passwords on an organization's existing OT requires significantly more work, we still recommend having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversary TTPs change. **FREE SERVICES AND REFERENCES:** CISA Bad Practices	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

1.3 Multi-Factor Authentication (MFA) PR.AC-7	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Brute Force (T1110) Remote Services - Remote Desktop Protocol (T1021.001) Remote Services - SSH (T1021.004) Valid Accounts (T1078, ICS T0859) External Remote Services (ICS T0822) **RECOMMENDED ACTION:** Hardware-based MFA is enabled when available; if not, then soft tokens (such as via mobile app) should be used; MFA via SMS should only be used when no other options are possible. **IT:** IT accounts leverage multi-factor authentication to access organizational resources. **OT:** Within OT environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendor/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible Human Machine Interfaces (HMIs). **FREE SERVICES AND REFERENCES:** CISA Bad Practices	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

1.4 Minimum Password Strength	PR.AC-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES

COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW

TTP OR RISK ADDRESSED:

Brute Force - Password Guessing (T1110.001)
Brute Force - Password Cracking (T1110.002)
Brute Force - Password Spraying (T1110.003)
Brute Force - Credential Stuffing (T1110.004)

RECOMMENDED ACTION: Organizations have a system-enforced policy that requires a minimum password length of 15* or more characters for all password protected IT assets, and all OT assets where technically possible.** Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement.

This goal is particularly important for organizations that lack widespread implementation of MFA and capabilities to protect against brute-force attacks (such as Web Application Firewalls and third-party Content Delivery Networks) or are unable to adopt passwordless authentication methods.

* Modern attacker tools can crack 8 character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations, and makes it easier for humans to create and remember passwords.

** OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as those on offshore rigs or on top of wind turbines.

FREE SERVICES AND REFERENCES: CISA Bad Practices, XKCD 936

CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
DATE:	DATE:	
☐ IMPLEMENTED	☐ IMPLEMENTED	
☐ IN PROGRESS	☐ IN PROGRESS	
☐ SCOPED	☐ SCOPED	
☐ NOT STARTED	☐ NOT STARTED	

1.5 Separating User and Privileged Accounts	PR.AC-4	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES

COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW

TTP OR RISK ADDRESSED:

Valid Accounts (T1078, ICS T0859)

RECOMMENDED ACTION: No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g. for business email, web browsing, etc.). Privileges are revaluated on a recurring basis to validate continued need for a given set of permissions.

CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
DATE:	DATE:	
☐ IMPLEMENTED	☐ IMPLEMENTED	
☐ IN PROGRESS	☐ IN PROGRESS	
☐ SCOPED	☐ SCOPED	
☐ NOT STARTED	☐ NOT STARTED	

1.6 Unique Credentials	PR.AC-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES

COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** MEDIUM

TTP OR RISK ADDRESSED:

Valid Accounts (T1078, ICS T0859)

Brute Force - Password Guessing (T1110.001)

RECOMMENDED ACTION: Organizations provision unique and separate credentials for similar services and asset access on IT and OT networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/machine accounts have unique passwords from all member user accounts.

CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
DATE:	DATE:	
☐ IMPLEMENTED	☐ IMPLEMENTED	
☐ IN PROGRESS	☐ IN PROGRESS	
☐ SCOPED	☐ SCOPED	
☐ NOT STARTED	☐ NOT STARTED	

1.7 Revoking Credentials for Departing Employees PR.AC-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Valid Accounts (T1078, ICS T0859) **RECOMMENDED ACTION:** A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely return all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

DEVICE SECURITY (2.0)

2.1 Hardware and Software Approval Process PR.IP-3	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Supply Chain Compromise (T1195, ICS T0862) Hardware Additions (T1200) Browser Extensions (T1176) Transient Cyber Asset (ICS T0864) **RECOMMENDED ACTION:** Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/ software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software, to include specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

2.2 Disable Macros by Default PR.IP-1, PR.IP-3	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Phishing - Spearphishing Attachment (T1566.001) User Execution - Malicious FIle (T1204.002) **RECOMMENDED ACTION:** A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

2.3 Asset Inventory ID.AM-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Hardware Additions (T1200) Exploit Public-Facing Application (T0819, ICS T0819) Internet Accessible Device (ICS T0883) **RECOMMENDED ACTION:** Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT. **FREE SERVICES AND REFERENCES:** Cyber Hygiene Services, or email vulnerability@cisa.DHS.gov, "Stuff Off Search" Guide, Validated Architecture Design Review (VADR); email central@cisa.gov	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

2.4 Prohibit Connection of Unauthorized Devices PR.PT-2	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** HIGH **TTP OR RISK ADDRESSED:** Hardware Additions (T1200) Replication Through Removable Media (T1091, ICS T0847) **RECOMMENDED ACTION:** Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling AutoRun. **OT:** When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices, or establish procedures for granting access through approved exceptions.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

2.5 Document Device Configurations PR.IP-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Delayed, insufficient, or incomplete ability to maintain or restore functionality of critical devices and service operations. **RECOMMENDED ACTION:** Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling AutoRun. **OT:** When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices, or establish procedures for granting access through approved exceptions.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

DATA SECURITY (3.0)

3.1 Log Collection — PR.PT-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Delayed, insufficient, or incomplete ability to detect and respond to potential cyber incidents. Impair Defenses (T1562) **RECOMMENDED ACTION:** Access and security focused (e.g., IDS/IDPS, firewall, DLP, VPN) logs are collected and stored for use in both detection and incident response activities (e.g. forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. **OT:** For OT assets where logs are non-standard or not available, network traffic and communications to and from log-less assets is collected. **FREE SERVICES AND REFERENCES:** Validated Architecture Design Review (VADR); email central@cisa.gov	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

3.2 Secure Log Storage — PR.PT-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Indicator Removal on Host - Clear Windows Event Logs (T1070.001) Indicator Removal on Host - Clear Linux or Mac System Logs (T1070.002) Indicator Removal on Host - File Deletion (T1070.004) Indicator Removal on Host (ICS T0872) **RECOMMENDED ACTION:** Logs are stored in a central system, such as a Security Information and Event Management (SIEM) tool or central database, and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines. **FREE SERVICES AND REFERENCES:** Validated Architecture Design Review (VADR); email central@cisa.gov	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

3.3 Asset Inventory — PR.DS-1, PR.DS-2	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Adversary-in-the-Middle (T1557) Automated Collection (T1119) Network Sniffing (T1040, ICS T0842) Wireless Compromise (ICS T0860) Wireness Sniffing (ICS T0887) **RECOMMENDED ACTION:** Properly configured and up-to-date transport layer security (TLS) is utilized to protect data in transit where technically feasible. Organizations should also plan for identifying any use of outdated or weak encryption and updating to sufficiently strong algorithms, and consideration for managing the implications of post-quantum cryptography. **OT:** To minimize the impact to latency and availability; encryption is used where feasible, usually for OT communications connecting with remote/external assets. **FREE SERVICES AND REFERENCES:** Validated Architecture Design Review (VADR); email central@cisa.gov	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

3.4 Secure Sensitive Data PR.DS-1, PR.DS-2, PR.DS-5	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Unsecured Credentials (T1552)Steal or Forge Kerberos Tickets (T1558) OS Credential Dumping (T1003) Data from Information Repositories (ICS T0811) Theft of Operational Information (T0882) **RECOMMENDED ACTION:** Sensitive data, including credentials, are not stored in plaintext anywhere in the organization, and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

GOVERNANCE AND TRAINING (4.0)

4.1 Organizational Cybersecurity Leadership ID.GV-1, ID.GV-2	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Lack of sufficient cybersecurity accountability, investment, or effectiveness. **RECOMMENDED ACTION:** A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

4.2 OT Cybersecurity Leadership ID.GV1, ID.GV-2	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Lack of accountability, investment, or effectiveness of OT cybersecurity program. **RECOMMENDED ACTION:** A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 4.1.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

4.3 Basic Cybersecurity Training PR.AT-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** User Training (M1017, ICS M0917) **RECOMMENDED ACTION:** At least annual trainings for all organizational employees and contractors that covers basic security concepts, such as phishing, business email compromise, basic operational security (OPSEC), password security, etc., as well as fostering an internal culture of security and cyber awareness. New employees receive initial cybersecurity training within 10 days of onboarding, and recurring training on at least an annual basis. **FREE SERVICES AND REFERENCES:** CISA Cyber Training	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

4.4 OT Cybersecurity Training PR.AT-2, PR.AT-3, PR.AT-5	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** User Training (M1017, ICS M0917) **RECOMMENDED ACTION:** In addition to basic cybersecurity training, personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training on at least an annual basis. **FREE SERVICES AND REFERENCES:** CISA ICS Training	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

4.5 Improving IT and OT Cybersecurity Relationships ID.GV-2	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Poor working relationships and a lack of mutual understanding between IT and OT cybersecurity can often result in increased risk for OT cybersecurity. **RECOMMENDED ACTION:** Organizations sponsor at least one 'pizza party' or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel, and is not a working event (such as providing meals during an incident response).	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

VULNERABILITY MANAGEMENT (5.0)

5.1 Mitigating Known Vulnerabilities	PR.IP-12, ID.RA-1, DE.CM-8, RS.MI-3	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Active Scanning - Vulnerability Scanning (T1595.002) Exploit Public-Facing Application (T1190, ICS T0819) Exploitation of Remote Service (T1210, ICS T0866) Supply Chain Compromise (T1195, ICS T0862) External Remote Services (T1133, ICS T0822) **RECOMMENDED ACTION:** All known exploited vulnerabilities (listed in CISA's KEV catalog - https://www.cisa.gov/known-exploited-vulnerabilities-catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first. **OT:** For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g. segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet, or reduce the ability of adversaries to exploit the vulnerabilities in these assets. **FREE SERVICES AND REFERENCES:** Known Exploited Vulnerabilities (KEV) Catalog, Cyber Hygiene Services, or email vulnerability@cisa.dhs.gov		DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

5.2 Vulnerability Disclosure/Reporting	RS.AN-5	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** LOW **COMPLEXITY:** HIGH **TTP OR RISK ADDRESSED:** Active Scanning - Vulnerability Scanning (T1595.002) Exploit Public-Facing Application (T1190, ICS T0819) Exploitation of Remote Service (T1210, ICS T0866) Supply Chain Compromise (T1195, ICS T0862) **RECOMMENDED ACTION:** Consistent with NIST SP 800-53 Revision 5, organizations maintain a public, easily-discoverable method for security researchers to notify (e.g. via email address or web form) organizations' security teams of vulnerable, mis-configured, or otherwise exploitable assets. Valid submissions are acknowledged and responded to in a timely manner, taking into account the completeness and complexity of the vulnerability. Validated and exploitable weaknesses are mitigated consistent with their severity. Security researchers sharing vulnerabilities discovered in good faith are protected under Safe Harbor rules. In instances where vulnerabilities are validated and disclosed, public acknowledgement is given to the researcher who originally submitted the notification. **FREE SERVICES AND REFERENCES:** Vulnerability Disclosure Policy Template, Disclose.io Policy Maker, Vulnerability Reporting; email vulnerability@cisa.dhs.gov, Coordinated Vulnerability Disclosure Process		DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

5.3 Deploy Security.txt Files	RS.AN-5	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Active Scanning - Vulnerability Scanning (T1595.002) Exploit Public-Facing Application (T1190, ICS T0819) Exploitation of Remote Service (T1210, ICS T0866) Supply Chain Compromise (T1195, ICS T0862) **RECOMMENDED ACTION:** All public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116. **FREE SERVICES AND REFERENCES:** https://securitytxt.org		DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

5.4 No Exploitable Services on the Internet PR.PT-4	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Active Scanning - Vulnerability Scanning (T1595.002) Exploit Public-Facing Application (T1190, ICS T0819) Exploitation of Remote Service (T1210, ICS T0866) External Remote Services (T1133, ICS T0822) Remote Services - Remote Desktop Protocol (T1021.001) **RECOMMENDED ACTION:** Assets on the public internet expose no exploitable services, such as RDP. Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets. **FREE SERVICES AND REFERENCES:** Cyber Hygiene Services, or email vulnerability@cisa.DHS.gov, "Stuff Off Search" Guide, Remote Penetrating Testing (RPT), Risk and Vulnerability Assessment (RVA)	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

5.5 Limit OT Connections to Public Internet PR.PT-4	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Active Scanning - Vulnerability Scanning (T1595.002) Exploit Public-Facing Application (T1190, ICS T0819) Exploitation of Remote Service (T1210, ICS T0866) External Remote Services (T1133, ICS T0822) **RECOMMENDED ACTION:** No OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.). **FREE SERVICES AND REFERENCES:** Cyber Hygiene Services, or email vulnerability@cisa.DHS.gov, "Stuff Off Search" Guide, Remote Penetrating Testing (RPT)	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

5.6 Third-Party Validation of Cybersecurity Control Effectiveness ID.RA-1, ID.RA-3	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** HIGH **TTP OR RISK ADDRESSED:** Reduce risk of gaps in cyber defenses or a false sense of security in existing protections. **RECOMMENDED ACTION:** Third-parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical (including OT/ICS) systems. High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests. **FREE SERVICES AND REFERENCES:** Remote Penetrating Testing (RPT), Risk and Vulnerability Assessment (RVA), Table Top Exercise Packages, Critical Infrastructure Exercises	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

SUPPLY CHAIN / THIRD PARTY (6.0)

6.1 Vendor/Supplier Cybersecurity Requirements	ID.SC-3	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Supply Chain Compromise (T1195, ICS T0862) **RECOMMENDED ACTION:** Organizations' procurement documents include cybersecurity requirements and questions, which are evaluated in vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred.		DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

6.2 Supply Chain Incident Reporting	ID.SC-1, ID.SC-3	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Supply Chain Compromise (T1195, ICS T0862) **RECOMMENDED ACTION:** Procurement documents and contracts, such as Service Level Agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed timeframe as determined by the organization.		DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

6.3 Supply Chain Vulnerability Disclosure	ID.SC-1, ID.SC-3	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Supply Chain Compromise (T1195, ICS T0862) **RECOMMENDED ACTION:** Procurement documents and contracts, such as Service Level Agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed timeframe as determined by the organization.		DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

RESPONSE AND RECOVERY (7.0)

7.1 Incident Reporting — RS.CO-2, RS.CO-4	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Without timely incident reporting, CISA and other groups are less able to assist affected organizations, and lack critical information into the broader threat landscape (such as whether a broader attack is occurring against a specific sector). **RECOMMENDED ACTION:** Organizations maintain codified policy and procedures on to whom and how to report all confirmed cybersecurity incidents to appropriate external entities (e.g. state/federal regulators or SRMA's as required, ISAC/ISAO, as well as CISA). Known incidents are reported to CISA as well as other necessary parties within timeframes directed by applicable regulatory guidance or in the absence of guidance, as soon as safely capable. This goal will be revisited following full implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). **FREE SERVICES AND REFERENCES:** Incident Reporting and/or contact report@cisa.gov or (888) 282-0870	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

7.2 Incident Response (IR) Plans — PR.IP-9, PR.IP-10	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Inability to quickly and effectively contain, mitigate, and communicate about cybersecurity incidents. **RECOMMENDED ACTION:** Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally-specific (e.g. by sector, locality, etc.) threat scenarios and TTPs. When conducted, tests or drills are as realistic in nature as feasible. IR plans are drilled at least annually, and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill. **FREE SERVICES AND REFERENCES:** Table Top Exercise Packages, Critical Infrastructure Exercises	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

7.3 System Back Ups — PR.IP-4	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Data Destruction (T1485, ICS T0809) Data Encrypted for Impact (T1486) Disk Wipe (T1561) Inhibit System Recovery (T1490) Denial of Control (ICS T0813) Denial/Loss of View (ICS T0815, T0829) Loss of Availability (T0826) Loss/Manipulation of Control (T0828, T0831) **RECOMMENDED ACTION:** All systems that are necessary for operations are regularly backed up on a regular cadence, no less than once per year. Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year. Stored information for OT assets includes at a minimum: configurations, roles, PLC logic, engineering drawings and tools.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

7.4 Document Network Topology PR.IP-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** MEDIUM **TTP OR RISK ADDRESSED:** Incomplete or inaccurate understanding of network topology inhibits effective incident response and recovery. **RECOMMENDED ACTION:** Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and OT networks. Periodic reviews and updates should be performed and tracked on a recurring basis. **FREE SERVICES AND REFERENCES:** Validated Architecture Design Review (VADR); email central@cisa.gov	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

OTHER (8.0)

8.1 Network Segmentation — PR.AC-5, PR.PT-4, DE.CM-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** HIGH **TTP OR RISK ADDRESSED:** Network Service Discovery (T1046) Trusted Relationship (T1199) Network Connection Enumeration (ICS T0840) Network Sniffing (T1040, ICS T0842) **RECOMMENDED ACTION:** All connections to the OT network are denied by default unless explicitly allowed (e.g. by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone (DMZ), which is closely monitored, captures network logs, and only allows connections from approved assets. **FREE SERVICES AND REFERENCES:** Validated Architecture Design Review (VADR); email central@cisa.gov	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

8.2 Detecting Relevant Threats and TTPs — ID.RA-3, DE.CM-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** HIGH **TTP OR RISK ADDRESSED:** Without the knowledge of relevant threats and ability to detect them, organizations risk adversaries existing in their networks undetected for long periods. **RECOMMENDED ACTION:** Organizations have documented a list of threats and adversary TTPs relevant to their organization (for example, based on industry, sectors, etc.), and have the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

8.3 Email Security — PR.DS-1, PR.DS-2, PR.DS-5	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** MEDIUM **COMPLEXITY:** LOW **TTP OR RISK ADDRESSED:** Phishing (T1566) Business Email Compromise **RECOMMENDED ACTION:** On all corporate email infrastructure (1) STARTTLS is enabled, (2) SPF and DKIM are enabled, and (3) DMARC is enabled and set to "reject." For further examples and information, see CISA's past guidance for Federal Agencies at https://www.cisa.gov/binding-operational-directive-18-01. **FREE SERVICES AND REFERENCES:** CISA Binding Operational Directive	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	