Implementation Guidance for Cybersecurity Performance Goals (Mandatory)

What is the SBIR/STTR Cybersecurity Requirement?

The Cybersecurity (CS) requirement is for applicants and awardees, who are interested in applying for a SBIR/STTR award, to fully implement 16 Cybersecurity Performance Goals (CPGs) listed on the SBIR/STTR Self-Assessment. The SBIR/STTR CPGs are a subset of the Cybersecurity Infrastructure Security Agency's (CISA's) CPG Checklist, however the language has been modified to reflect additional clarification and guidance for DOE SBIR/STTR specific CPG requirements. Overall, the SBIR/STTR CPGs intend to be:

- A baseline set of CS best practices that have been prioritized for SBIR/STTR Small Businesses.
- A benchmark for SBIR/STTR Small Businesses to measure and improve their CS maturity.
- A unique security control framework intended to address risks associated with SBIR/STTR Small Businesses.

The applicants and awardees are encouraged to review the framework to understand how to develop and implement cybersecurity within their small business. In addition, NIST has developed helpful resources to support small businesses establish and/or improve their CS which can be found here: Small Business Cybersecurity Corner | NIST. Another resource highly recommended for small businesses is the Global Cybersecurity Alliance (GCA) site which provides CS training and tools that can help applicants and awardees implement the required CPGs. In addition, this implementation guidance leverages the GCA sites which offer useful tools training videos and checklists/templates centered around small businesses. The GCA Learning Portal link is Understanding Cyber Risk for Small Business (globalcyberalliance.org) The GCA toolkit link is: GCA Cybersecurity Toolkit for Small Business | Sponsored by Mastercard (gcatoolkit.org)

This implementation guidance also references and utilizes the Department of Homeland Security (DHS) Cyber Resilience Review (CRR) Resource Guides. These resource guides provide instructions on CS best practices that can support the implementation of the required CPGs. The CS best practices mentioned in the DHS CRR Guides are based on the CERT Resilience Management Model (CERT®-RMM), a maturity model for managing and improving operational resilience. In addition, CS resources from CISA and the Federal Trade Commission were also used in this implementation guidance.

What are the requirements of the SBIR/STTR CPGs?

- 2.L Secure Sensitive Data (Critical): The small business should protect sensitive information from unauthorized access.
- 2.E Separate User and Privileged Accounts (Critical): The small business should make it harder for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised.
- 2.D Revoke Credentials (Critical): The small business should prevent unauthorized access to organizational accounts or resources by former employees
- 1.B Organizational CS Leadership (Critical): The small business should identify a leader who is responsible and accountable for cybersecurity within an organization.
- 2.I Basic CS Training: The small business' workforce should be trained in cybersecurity and be able to support CS best practices.
- 1.A Asset Inventory (Critical): The small business should create an asset inventory to identify authorized/unauthorized use of any digital service or device that is not formally approved and supported by the IT department, unmanaged/managed assets, and helps to rapidly detect and respond to new vulnerabilities.
- 2.A Change Default Passwords (Critical): The small business should prevent threat actors from using default passwords to achieve initial access or to move laterally in a network.
- 2.R System Backups (Critical): The small business should secure data and reduce the likelihood/duration of data loss during loss of service, delivery, or operations.
- 2.B Minimum Password Strength: The small business should create and use complex passwords that are harder for threat actors to guess or crack.
- 2.H Phishing Multi-Factor Authentication (MFA): The small business should include additional layer(s) of security to protect assets accounts whose credentials have been compromised.
- 2.W No Exploitable Services: The small business should identify and monitor all assets, especially public-facing assets, and ensure unauthorized users cannot gain an initial system foothold by exploiting known weaknesses.
- 2.G Detection of Login Attempts: The small business should protect its assets from automated, credential-based attacks.
- 2.K Strong and Agile Encryption: The small business should deploy effective encryption to maintain confidentiality and integrity of sensitive data being processed, in transit or at rest.
- 2.M Email Security: The small business should reduce risk from common email-based threats, such as spoofing, phishing, and interception.
- 2.S Incident Response Plan: The small business should develop, document, maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.

- 4.A IR Reporting: The small business should have security incident reporting procedures to contact an internal incident response team and/or senior management. In addition, the small business should have available the contact information of CISA, FBI, or local police for assistance with security incidents or to understand the broader scope of a cyberattack.

More information regarding the requirements to fully implement these CPGs can be found in the CPG Implementation Guidance section of this document, however, applicants and awardees should review the guidance in its entirety to better understand how the guide works and for the additional information/resources available to support CPG implementation.

What are the options to implement the CPGs?

To clarify, the CS Due Diligence Program will not provide CS solutions for SBIR/STTR applicants and awardees, however, the program will provide suggestions on how to implement the required CPGs and assist with questions and concerns regarding the DOE SBIR/STTR CS requirement. The applicants/awardees are responsible for developing their CS solutions and to meet full implementation of the 16 CPGs. Below are some options for how to implement the CPGs in order of highest to lowest complexity. The DOE SBIR/STTR CS Due Diligence Program is not directing/recommending small businesses to use a particular option, we are providing suggestions that can help small businesses implement the CPGs. It is the responsibility of small businesses to review, understand and fully implement each CPG, regardless of what option(s) is/are used to implement the CPG.

First Option:

The SBIR/STTR Applicants and Awardees may fully implement the 16 required CPGs by reviewing the **Implementation Guidance for the Required CPGs** section and following the recommended implementation guidance provided. If this option is selected, then the small business will be provided some online tools and information to assist with implementation of the CPGs. This option is the most complex and time consuming for the applicants and awardees. Some of the CPGs may require some technical expertise to implement so if you're a small business that lacks the CS expertise, then you may want to review the other options mentioned below.

Second Option:

Another way for the SBIR/STTR Applicants/Awardees to address the full implementation of the required CPGs is to research the security features offered by Cloud platform, such as Microsoft Azure, Google, Aws, etc. These Cloud platforms may allow businesses access to free technical tools, such as remote services, email security, etc. which can be useful at securing the daily operations of a business. In addition, some Cloud Platforms may offer security features (at no additional cost) that can be enabled and assist in the partial and/or full implementation of CPGs. To clarify, the DOE SBIR/STTR Programs does not require or recommend that SBIR/STTR small

CPG	Google Workspace	Microsoft Office 365	Zoho Workplace
1.B Organizational CS Leadership	Business Defined	Business Defined	Business Defined
1.A Asset Inventory (Critical)	Business defined, however, services/tools to complete this CPGs may be offered.	Business defined, however, may provide asset management service.	Business defined, however, services/tools to complete this CPGs may be offered.
2.A Change Default Passwords (Critical)	User Controlled	User Controlled	User Controlled
2.L Secure Sensitive Data (Critical)	**Service Provided**: 2-Step Verification, passkeys, and security keys, Single Sign-On (SSO), OAuth 2.0, and SAML support. Real-time, risk-based re-authentication security feature may be available. Automatic spam, phishing, and malware defenses could also be available. Endpoint management of mobile and desktop devices and encryption of data in transit and at rest could also be available.	**Services Provided**: BitLocker, Transport Layer Security (TLS) Protocol, emails between two recipients- S/MIME, TLS Microsoft teams TLS and MTLS to encrypt instant messaging, Media traffic is encrypted using secure RTP (SRTP). Federal information processing standard (FIPS).	**Services Provided**: Encryption in transit (TLS), encryption at rest, Application-level encryption, Full-disk encryption.
2.R System Backups (Critical) Microsoft	Service Provided: GoogleDrive	Service Provided: OneDrive	Service Provided: Zoho WorkDrive
2.B Minimum Password Strength	Service provided: enforce and monitor password requirements for users.	Service Provided: Create Password Polices.	Service provided: configure password policy
2.W No Exploitable Services	Service Provided: Google workspace Admin	Service Provided: Access control list (ACL)	Service provided: User access control
2.K Strong and Agile Encryption	Services is provided	Service is provided	Service is provided
2.I Basic CS Training	Business Defined	Business defined	Business defined
2.E Separate User and Privileged Accounts	Service Provided: Access Management	Service Provided: Control access to business information with security groups and custom permissions. Restrict access to sensitive business information with information rights management	Role-based access control (RBAC)

2.D Revoke Credentials	Business Defined	Admin Center	Business Defined
2.H Phishing Resistant MFA	Services Provided: 2FA, Single sign-on (SAML 2.0), OAuth 2.0 and OpenID Connect	Services Provided: Secure access with multifactor authentication	
2.M Email Security	Services Provided: Can implement DMARC by creating a DMARC record within their admin settings and implementing an SPF record and DKIM keys on all outbound mail streams.	Services Provided: Emails between two recipients- S/MIME. malware with cloud-based email filtering	Services Provided: Encrypted message content, digital signatures, and encryption services, S/MIME prevents email attacks, data leaks, phishing, and email spoofing
2.G Detection of Login Attempts	Services Provided: Information Rights Management (IRM)	Services Provided: Microsoft 365 Reports	May provide service
2.S Incident Response Plan	Business Defined	Business Defined	Business Defined
4.A IR Reporting	Services Provided: Cyber Incident Response Service	Services Provided: Microsoft Incident Response	Services provided: incident management software

businesses utilize Cloud platforms to address the full implementation of the required CPGs, but only provides a suggestion on how the small businesses can meet full implementation of the required SBIR/STTR CPGs. The small business is ultimately response for ensuring the SBIR/STTR CPG requirements are fully implemented. Before contacting the IT service provider, the applicants and awardees should understand the SBIR/STTR CPG requirements in the **Implementation Guidance for the Required CPGs section** of this document. Below is a list of cloud service providers that may be able to assist SBIR/STTR applicants and awardees with the partial and/or full implementation of the CPGs.

Third Option:

A Managed Security Service Provider (MSSP) and/or Managed Service Provider (MSP) could also assist small businesses with the full implementation of the required CPGs. The SBIR/STTR Applicants and Awardees should understand the SBIR/STTR CPG requirements in the **Implementation Guidance for the Required CPGs section** of this document before contacting a MSSP or MSP. A MSSP is a third-party provider (outsourced service) that manages and monitors a small business' security systems and devices (i.e. firewalls, virus protection, and intrusion detection) and ensures access is only for authorized personnel. The MSSP focuses on providing network security and IT safety. The MSP is also a third-party provider (outsourced service) that differs from a MSSP as it provides general IT support and services for small businesses that do

not have their own IT departments. Some MSPs manage the overall IT infrastructure allowing the small business to have more operational control over their IT systems. To clarify, the DOE SBIR/STTR Program does not require or recommend that SBIR/STTR small businesses employ an MSSP or MSP to meet full implementation of the required CPGs, but only provides a suggestion on how the small businesses can meet full implementation of the required SBIR/STTR CPGs. The SBIR/STTR Small Businesses are responsible for understanding the requirements for each CPG and ensuring that each CPG is fully implemented. Please visit the NIST Small Business CS Corner: Choosing a Vendor/Service Provider | NIST to learn more about choosing the right vendor/service provider for you.

Fourth Option:

One way to address the full implementation of the SBIR/STTR CPGs is to employ a CS Consultant, however, before contacting a CS consultant, applicants and awardees should understand the SBIR/STTR CPG requirements by reviewing the **Implementation Guidance for the Required CPGs section** of this document. The CS Consultant is a subject matter expert on CS and should be able to assist the small business with identifying the threat environment and vulnerabilities associated with their current business operations. The CS Consultant can help determine how the CPGs could be implemented and support business objectives. The CS Consultant should have extensive knowledge of the methods to fully implement the SBIR/STTR CPG requirements and the ability to tailor those efforts to the small business. To clarify, the DOE SBIR/STTR Programs do not require or recommend that SBIR/STTR Small Businesses employ CS Consultants to meet full implementation of the required CPGs, but only provides this information as a suggestion on how the small businesses can meet the full implementation of the required SBIR/STTR CPGs. The SBIR/STTR Small Businesses are responsible for understanding the requirements for each CPG and ensuring that each CPG is implemented.

Introduction to the CPG Implementation Guidance

The implementation of the CPGs is imperative to protect SBIR/STTR businesses from cyber criminals and attacks. Some of the challenges SBIR/STTR Small Businesses encounter are limited finances, lack of IT/CS experience, implementation of CS practices can be complex, untrained staff CS practices, reliance of third-party vendors with weak security practices and meeting compliance with state regulations (if applicable). Because small businesses are major targets for cyberattacks, the implementation of the CPGs should begin at the early stages of development. As the business/technology grows specific CPGs may need to be prioritized to address threats, such as, phishing and ransomware.

Keep in mind the size of the small business matters. Methods to fully implement the CPGs will differ between a small business that has 1-10 employees compared to a small business that has 50-100 employees to business that have up to 500 employees. The CPG requirement does not change based on the size of the business; however, the implementation of the CPG will vary. Factors such as, the number of assets (systems, personnel, devices, etc.) and types of technologies used to monitor assets and perform daily operations, location of high critical assets/high value assets, and impact to the business if a cyberattack was successful should be considered when deciding on the full implementation of the CPGs. The SBIR/STTR

Applicants/Awardees should consider the following before choosing how to implement the CPGs, (but, not limited to):

- How does the business operate to meet its mission/objectives? Review and identify current business practices and applications used (i.e., online research, collaborating with other stakeholders on MS Teams, etc.). Also, what technologies do you use (tablet, cell phones, etc.)? This information is helpful in determining how and where the data is developed, stored, and transmitted, as well as, who has access to the data.
- Do you have a documented process that instructs employees on how and when employees should classify intellectual property and/or sensitive data? Does your documentation identify where this information should be stored and who should have access? By classifying data, you can then identify, monitor, and secure the assets that develop, process, stores, and/or transmits the information (including interconnections to other assets).
- Data drives the priorities. Sensitive data/intellectual property with its associated systems/assets are considered critical to a small business and are considered 'high value assets' (HVAs) or can be known as critical assets. The HVAs/critical assets should drive the prioritization of the CPG implementation to ensure the confidentiality, integrity, and availability of the information is protected. Consider if there is an unauthorized disclosure of sensitive information and/or intellectual property, what would the impact be for the small business? For most SBIR/STTR Small Businesses this would have a devastating impact. Reviewing the factors above may assist SBIR/STTR Applicants/Awardees with identifying their HVAs, understand the impact if they are compromised, determine level of risks, and assist in the development of an implementation plan for the required CPGs.

What are Critical CPGs?

The SBIR/STTR CS Due Diligence Program has prioritized the implementation of the required 16 CPGs. There are CPGs that have been identified as 'critical' and are fundamental in the initial implementation of CPGs. Implementing the critical CPGs first ensures that the small business addresses the appropriate scope (high value/critical assets) and develops an implementation plan aligned to the small business efforts/mission. In addition, the implementation guidance reflects how the CPGs are related and interdependent. If the critical CPGs are not implemented first, then the small business will be deemed a 'High Risk.' Please refer to the Risk Rating Information page for a **full** description of all risk ratings. *Note:* ***Full implementation of ALL 16 CPGs is highly recommended prior to application submission.***

The Critical CPGs discussed above are: 2.L Secure Sensitive Data, 2.E Separate User and Privilege Accounts, 2.D Revoke Credentials, 1.B Organizational CS Leadership, 1.A Asset Inventory, 2.A Change Default Passwords, and 2.R System Backups

Structure of the CPG Implementation Guidance:

What DOE SBIR/STTR CS Self-Assessment CPG(s) is/are being met?

This section identifies the applicable CPG(s) and displays the actual language found on the DOE SBIR/STTR CS Self-Assessment. Note: The language in this section has been modified from the CISA CPG Checklist to reflect additional clarification and guidance for DOE SBIR/STTR specific CPG requirements.

What is required to implement the CPGs?

This section of the guidance will provide the resources required and information to implement the CPG. As mentioned earlier, the SBIR/STTR Program will be utilizing the free online Global Cyber Alliance (GCA) Toolkit to assist small businesses with the implementation of the required CPGs.

- All SBIR/STTR applicants/awardees should visit and familiarize themselves with the GCA Toolkit for Small Business at this link: GCA Cybersecurity Toolkit for Small Business | Sponsored by Mastercard (gcatoolkit.org)
    - All SBIR/STTR applicants/awardees should scroll down on the left side of the main screen, click on 'Resources' and view the video, 'How to Use the Toolkit' to learn how this resource should be used (about a 16-minute video).
    - All SBIR/STTR applicants/awardees are highly encouraged to register for a free account on the GCA Learning Portal which can be found on the homepage or at this link: https://edu.globalcyberalliance.org/
        - The GCA Learning Portal has useful tools, training videos and checklists/guides that give a brief introduction of the threats, risks, and explain methods to implement CS best practices/CPGs to ensure your small business is protected.
        - The tools, training videos and checklists/guides mentioned above will be required and part of the SBIR/STTR implementation guidance.

The implementation guidance below may suggest that you watch a short training presentation from the GCA Learning Portal and then download the applicable tool(s) and/or checklist/guide to fully/partially implement the CPGs. The development of policies to support the CPGs is also suggested, however, ultimately the applicants/awardees will have to determine if it is applicable based on the number of systems, employees, risk appetite, etc. However, the processes that support the CPGs should be documented by the applicants/awardees and is highly recommended. In addition, other applicable resources from DHS, CISA and NIST, etc. will also be listed to aide with the CPG implementation.

CPG Implementation Guidance (broken down by CPGs)

What DOE SBIR/STTR CS Self-Assessment Requirements are being met?

2.L Secure Sensitive Data (Critical): The small business should protect sensitive information from unauthorized access.

The overall goal of implementing all the required CPGs is to 'Secure Sensitive Data' (information/intellectual property)' of small businesses from unauthorized disclosure. However, as

part of implementing this 'critical' requirement (Secure Sensitive Data), small businesses should fully implement 2.E Separating User and Privileged Accounts and 2.D Revoke Credentials.

2.E Separating User and Privileged Accounts: The small business should make it harder for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised.

2.D Revoke Credentials: The small business should prevent unauthorized access to organizational accounts or resources by former employees

What is required to implement these CPGs?

To fully implement Separating User and Privileged Accounts and Revoke Credentials, the SBIR/STTR Applicants and Awardees should develop and implement the processes to restrict access to sensitive information and intellectual property to only authorized users. The processes should be documented, reviewed/updated regularly, and stored in a secure location.

1. Small businesses should leverage built-in access management on existing platforms. Google Workspace and Microsoft 365 have built-in user access management features within the basic plan. This will allow you to assign roles, control permissions and enable multi-factor authentication (MFA) for minimal cost. In addition, small businesses can manage access to file storage and collaboration on platforms like Dropbox and Google Drive. If using cloud services providers such as, AWS, Azure and Google Cloud Platform, then take advantage of the Identity and Access Management (IAM) features (again) at no extra cost. If these features are properly configured the small business will be able to control access over specific resources, such as, critical assets.
2. Restricting administrator-level access is suggested to minimize the damage in case of a compromised user account. Applicants and awardees should restrict access to sensitive data/resources by only giving employees access to data necessary for their roles.
    a. The applicants/awardees should also review the NISTIR 7316 to learn more about access control and the different models, as well as their capabilities/limitations. This will require IT/CS technical expertise when implementing. Applicants may select an access control model to properly configure their systems and control access to their critical assets/data.
        i. Access control list and access list are ways for applicants to control access to resources. Here are some access control models to consider:
            a. Discretionary Access Control (DAC): On operating systems, such as Microsoft, a Discretionary Access Control List (DACL) can be created which is a list of users or groups who are permitted access to certain resource(s) and assigns their type of access.
            b. Mandatory Access Control (MAC): This involves an individual assigned a clearance level such as, Unclassified, Secret, and Top Secret. The small business' assets/resources are also assigned classification labels based on the sensitivity of the information. The

operating systems controls access to the assets/resources by validating the clearance level. In addition, a high clearance level allows users access to resources/assets at the lower levels.

i. Role/Rule Based Access Control:

1. Role: The system assigns privileges to different roles. Users are given a role and belong to a group with assigned privileges to perform the task. Everyone in that role/group has the same privileges. Note: The privileges are assigned to role/group. This can be implemented with some project management software, such as Trello, Asana, etc. at no additional costs. Example of RBAC is designating one person as the 'administrator role' and all others are 'user' roles. The roles provide the access/functions needed for the role.

2. Rule: Involves configuring rules on the system or device, such as a firewall or router which could permit or not allow different actions to take place. Rules determine if what actions are allowed or not allowed to occur based on the configured device.

3. Questions to consider when developing access controls. What are the different roles in your small business? Do all roles require the same level of access? Are there roles that require a higher level of access? Are there some roles that may create a conflict of interest if performed by the same person?

ii. Where is the sensitive information or intellectual property that should be restricted to only certain roles/accounts/personnel? Identify critical assets that need to be protected (systems/devices that store sensitive data like financial and personnel data, intellectual property, etc.).

b. When assigning permissions, Separation of Duties (SoD) and Least Privilege are two core access control principles that can help minimize the risk of unauthorized disclosure:

i. Separation of Duties (SoD) is a security and internal control principle that involves division of critical tasks among different individuals or teams to reduce the risk of fraud, error or misuse of resources. By ensuring that no single person has control over all aspects of a task, it minimizes the opportunity for unethical behavior or mistakes. Note: This is a compensating

control that small businesses (especially those who have 1-5 employees) can implement to protect against theft, insider threat, and fraud.

ii. Principle of Least privilege: This is based off the practice of granting users, systems, or processes only the minimum level of access or permission necessary to perform their tasks. This helps minimize security risks by reducing the potential damage that could occur if an account or system is compromised. idea that minimal permissions to complete the task should be assigned to each user. With minimal permissions, users are limited to what is required for the task. This ensures that personnel are limited to essential actions and information on critical asset (restricting access to administrator-level).

3. Another suggestion is for applicants and awardees to review the NIST CSF v2.0 Small Business Quick Start Guide, specifically the 'Protect Function' to understand how to safeguard their critical assets/sensitive data and how it fits within a CS framework. In addition, the NIST CSF 2.0 Implementation Examples can assist with developing their processes. Review 'Protect (PR)' section and implement the CPG by using the examples provided. As a reminder, the level of protection required to keep sensitive data safe is determined by the small business.

4. Applicants and awardees should also review the 'document released by CISA and National Security Agency (NSA) to learn how to limit access of critical assets/data to only authorized personnel by managing the identity and access of personnel. The first five pages provides some best practices that can be used to mitigate the activities that threat actors commit when exploiting known Identity and Access Management (IAM) vulnerabilities.

5. Another suggestion for applicants and awardees to ensure data is restricted to only authorized personnel is to develop an auditing process that involves routine reviews of users with privileged accounts. The periodic reviews should validate all personnel who have access to sensitive data. If user access is invalid, then the access should be adjusted.

6. When developing and documenting the privileged access process, below are things to consider:

    a. Create a centralized access list (as described in the previous CPG) of all employee access points (email, cloud platforms, SaaS tools) using tools like a spreadsheet or an identity management platform (e.g., Okta, JumpCloud).

    b. Develop, document and maintain a (manual or automated) process to deactivate accounts of departing employees on their last working day, to include processes to remove email, cloud, and internal system access. When developing the process, here are some things that should be addressed, but not limited to are:

        i. When to create, how to manage and disable privileged/user, new, temporary, and terminated employee accounts and credentials. This should include remote workers.

ii. What is the process to delete/disable accounts and/or revoking credentials on critical assets?

iii. How often are the criteria for privileged accounts and list of privileged users reviewed?

iv. Who are assigned users and privileged accounts and their roles/responsibilities? Do any of these roles present a conflict of interest?

v. When is separation of duties established and enforced? What roles should have separation of duties?

vi. How is remote access established and managed on critical assets? (if applicable)

1. Lastly, (if applicable) develop policy to support access management and the revocation of credentials processes, then download and complete the GCA Access Management Policy Template.

What DOE SBIR/STTR CPGs are being met?

1.B - Organizational Cybersecurity Leadership (Critical CPG): The small business should identify a leader who is responsible and accountable for CS within an organization.

2.I - Basic Cybersecurity Training: The small business' workforce should be trained in CS and be able to support CS best practices.

What is required to implement the CPG?

To fully implement the Organizational CS Leadership CPG, the applicants/awardees should assign a leader who is responsible for CS within the organization and has developed a plan to fully implement the required CPGs. To fully implement the Basic CS Training CPG, the CS leader should also document, develop, maintain and implement a training plan/program which includes basic security concepts associated with the required CPGs, as well as, how the workforce will be trained to support the protection of the small business computer systems, data and personnel from cyberattacks.

1. Applicants and awardees should assign a CS point of contact. This could be an internal staff member or an external consultant. If no one on staff is qualified, consider outsourcing to a Managed Security Service Provider (MSSP).

2. The assigned CS leader should develop a plan to implement the required SBIR/STTR CPGs and processes/policies that address passwords, access management, and how to handle data breaches, etc.

3. Below are suggestions to assist the leader with establishing and monitoring CS within the organization:

    a. Develop a cybersecurity and risk plan/process by meeting regularly to identify and assess IT-related risks. The following factors should be considered, but are not limited to:

i. Identification of high value assets (HVAs), their owners and dependencies. (What is the threat environment for HVAs, personnel and dependencies?)

ii. Identification of roles and responsibilities (internal/external) of CS efforts. (Who is responsible for risk identification, assessment, response/mitigation and continuous monitoring of risk?)

iii. Identification and process to addresses legal/regulatory requirements. (Are there any state/federal legal/requirements that need to be met?)

b. Please refer to the NIST CSF v.2 Small Business Quick Start Guide for more details on how to establish CS governance and view related Training: Foundations of Cybersecurity for Managers (usalearning.gov) and Cloud Security – What Leaders Need to Know (usalearning.gov)

4. Below are suggestions to assist the leader with developing a basic CS training program:

a. Develop, document, and disseminate within the organization basic security concepts of the threats associated with your small business, such as, social engineering (phishing) viruses, adware, etc.

b. Ensure new employees should receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.

c. A free basic CS training video is available for your small business through the Global Cyber Alliance Learning Portal: https://edu.globalcyberalliance.org. Review the training called, 'Protect Against Email Spoofs & Phishing' to learn more about Phishing and Spoofing.

d. There is also free NIST training available: Free and Low Cost Online Cybersecurity Learning Content | NIST and Cybersecurity Essentials fedvte.usalearning.gov

What is the DOE SBIR/STTR CS Self-Assessment Requirement?

1.A Asset Inventory (Critical): The small business should create an asset inventory to identify authorized/unauthorized use of any digital service or device that is not formally approved and supported by the IT department, unmanaged/managed assets, and helps to rapidly detect and respond to new vulnerabilities.

What is required to implement the CPG?

This CPG will take the most time to implement because of the amount of research and detail required, however, if implemented properly the small business will have a centralized repository of all assets which promotes a more efficient and effective way to protect against cyber-attacks, such as the unauthorized disclosure of sensitive information/intellectual property.

To fully implement this CPG, the SBIR/STTR Applicant and Awardee should develop, document, maintain and share with stakeholders a process of identifying and tracking assets, especially high value assets and creating an asset inventory that will be (1)used to identify authorized/unauthorized

use of any digital service or device this not approved/supported, managed/unmanaged by the IT department and able to assist with rapid detection and response to vulnerabilities.

1. Below are suggestions on how to develop an asset inventory and asset management process:

    a. Register and/or log into the GCA Learning Portal: https://edu.globalcyberalliance.org/ and view the free training presentation, "How to Inventory Your Devices, Apps, and Accounts." on the GCA Learning Portal to learn more about the importance of an asset inventory.

    b. Download and complete the 'Know What You Have Checklist' to learn what assets need to be identified, documented and maintained within your business.

    c. Understanding the data that you are processing, storing and transferring helps identify where critical assets are located, who has access to the critical assets and vulnerabilities. To help your workforce identify, classify and label sensitive data and intellectual property, download and complete the 'Data Classification' policy template.

2. After reviewing the free training and internal research has been done (steps above), then create an asset inventory by downloading and completing the 'CIS Hardware and Software Asset Training Spreadsheet' found on the GCA Learning Portal: https://edu.globalcyberalliance.org/. Be sure to include (but not limited to):

    a. All devices that are managed or not managed by your small business. (i.e. third-party service providers) and authorized/unauthorized.

    b. Known vulnerabilities and statuses.

    c. Who is responsible for the asset(s).

3. Download the GCA Asset Inventory & Device Management Policy template for assistance with developing and documenting an Asset Management Policy. If needed, download the DHS, CRR Supplemental Resource Guide, Volume 1 Asset Management (DHS, CRR AM) guide for more information on developing an Asset Management process that will align with the Asset Inventory & Device Management Policy.

    a. The following questions should be considered when developing your process/policy. See the DHS, CRR guide for more information.

        i. Who is responsible for developing, maintaining and updating the asset inventory?

        ii. How is continuous monitoring of the asset inventory conducted?

        iii. How are security incidents affecting critical assets communicated to senior management?

        iv. What services are identified and prioritized, especially if a security incident were to occur?

v. How are assets inventoried, and the authority and responsibility for these assets established?

vi. What is the relationship between assets and the services (dependencies)?

vii. How is the asset inventory managed when assets are implemented, shared and maintained (Patching Policy).

viii. How access managed, documented and shared with appropriate stakeholders.

ix. Where does the assets supporting the critical services reside and how they are prioritized and managed?

4. Lastly, developing an asset inventory and management process is aligned under the NIST CSF v2.0, 'Identify' function. The Identify Function is used to assist small businesses determine the current CS risk to the business based on the identified assets. Examples on how to implement the Identify Function, such as assessing assets for potential vulnerabilities and can be found on the NIST CSF 2.0 Implementation Examples under ID..AM.

5. If additional information about creating an asset inventory is required, then view related training: Related Training: Cover Your Assets! – Securing Critical and High-Value Assets (HVAs) (youtube.com), Critical Assets and Operations (usalearning.gov), Network Mapper | CISA

What is the DOE SBIR/STTR CS Self-Assessment Requirement?

2.A Change Default Passwords (Critical): The small business should prevent threat actors from using default passwords to achieve initial access or to move laterally in a network.

What is required to implement the CPG?

To fully implement this CPG, applicants/awardees should create, document and implement processes to change default passwords on all systems, software and services identified in your asset inventory. This includes developing a process that addresses critical assets that do not allow the default words to be changed. The processes should be disseminated to all stakeholders.

1. Conducting a vulnerability scan is recommended prior to changing default passwords. This helps identify vulnerabilities (known weaknesses), such as default passwords that haven't been changed on devices, software, or applications. These vulnerabilities can be easily exploited by threat actors and cause significant damage to a small business. Conducting vulnerability scans requires IT/CS technical expertise to run the scan with the proper scope, interpret the results, and mitigate the vulnerabilities, especially high or moderate vulnerabilities, such as changing default passwords.

    a. Applicants and awardees can contact CISA for free vulnerability scanning for SBIR/STTR Small Businesses working with DOE. Please see PDF: CISA Services for the DOE Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR)

i. If applicants/awardees use Apple, Android, or Microsoft products, they can learn about conducting vulnerability scans and setting up scan updates by logging into the GCA Learning Portal at https://edu.globalcyberalliance.org/courses/Understanding-Cyber-Risk and downloading the PDF Update Your Defense Checklist for completion.

ii. Use the information under 'Make Prompt Software Updates a Standard Practice' in the Update Your Defense Checklist to help create the required processes (or policies, if applicable).

b. Another option for applicants/awardees to learn more vulnerability scanning and help develop processes is to review: Understanding Patches and Software Updates | CISA

2. After the vulnerability scans have been performed default passwords that need to be changes are identified, then applicants and awardees should make the change and document it, as part of asset management process (see asset inventory). Below is more helpful information regarding changing default passwords that are suggested to help develop the processes needed to fully implement the CPG.

    a. Applicants and awardees should review the CISA Alert Code: TA13-175A Risks of Default Passwords on the Internet at this link: https://www.cisa.gov/news-events/alerts/2013/06/24/risks-default-passwords-internet

        i. One suggestion is to force default password changes; however, this process will require IT/CS expertise. Microsoft users can disable default accounts and enforce users to change default passwords when new devices are added to the network by configuring the default domain password policy.

        ii. After the default password policy has been set, it is also suggested to configure the systems to have unique, strong password requirements for all users under the default domain password policy. For more information on how to set up a strong unique password, then please refer to CPG B - Minimum Password Strength and/or view the related training: More than a Password | CISA and Cyb3R_Sm@rT!: Use a Password Manager to Create and "Remember" Strong Passwords | CISA

        iii. Another suggestion is to restrict network access to only trusted hosts and networks, especially for systems that do not allow default password changes. An access control list can restrict user access to critical assets, and firewall policies can be created to control traffic from personal devices and networks to only approved sources.

3. When documenting the default password process/policy, the following points are suggested (but not limited to):

a. Explain how default words are validated after they have been changed and how this part of the asset management process.

b. Describe the process for continuously monitoring default passwords.

c. Explain how unique, strong passwords are validated.

d. Outline mitigation plans for critical systems that do not allow default passwords to be changed.

e. Detail the process of conducting vulnerability scans to identify default passwords. The GCA Patching Policy Template can be used to document the vulnerability patching procedure.

What is the DOE SBIR/STTR CS Self-Assessment Requirement?

2.R System Backups (Critical): The small business should secure data and reduce the likelihood/duration of data loss during loss of service, delivery, or operations.

What is required to implement the CPG?

To fully implement this CPG, applicants/s should develop, test, document and implement processes which ensures the replication of information to a redundant system, service, device or medium and has the capability to restore when needed.

Before backing up systems, it is suggested that applicants/awardees conduct vulnerability scans on systems/devices and address all known vulnerabilities. Configuring back-up and restore feature may require the IT/CS technical expertise. Also, listed below are available training/information for applicants/awardees to learn more about system backups:

1. To learn more about backup methods, to include full backups, incremental backups (copying only changed data since that last backup), or differential backups (copying changed data since the last full backup) then download and review Data Backup Options (cisa.gov)

2. Log into the Global Cyber Alliance https://edu.globalcyberalliance.org/ and review the training video called, 'Protecting Your Data with Backups' to learn how to set up backups and restore capability to protect systems from data loss.

    a. To assist applicants and awardees with implementing system backups:

        i. Download and complete the 'Defend Against Ransomware: Backup & Recovery Checklist' from the GCA learning portal.

        ii. Utilize the GCA Cybersecurity Toolkit to install a free tool to set up automatic backups for MAC and MS Operating Systems

3. Google Drive, Microsoft OneDrive or Dropbox users can implement this CPG by using Cloud-based back up services (if applicable). The service may be an additional cost to use, however, it should provide ample secure storage for most small businesses.

4. Microsoft Azure, AWS, or Google Cloud Platform may offer built-in backup solutions that can automate backups across multiple services.
5. Windows and macOS users may also have built-in backup tools that are free and easy to setup. These tools may be able to backup to external drives and be a cost savings to small businesses.
6. Here are some factors to consider when documenting the system backup processes/policy:
    a. Use an alternate offsite backup storage solution, such as external hard drives, network-attached storage (NAS), cloud storage, or dedicated backup servers.
    b. For recovery purposes, ensure that the alternate storage site provides security controls equivalent to that of the primary site.
    c. Automate backup processes to ensure regular and consistent backups without manual intervention. (if applicable).
    d. Test backups periodically to verify their integrity and ensure they can be restored successfully in case of a data loss event.
    e. Identify who is responsible for backup and recovery and how often they are performed on critical assets?
    f. Identify critical data, applications and system configurations (from asset inventory) that should be backed up regularly.
    g. Configure system to back up and restore on MS Windows, macOS, IOS, Android.
    h. Identify who has physical access to data storage media and devices.
7. Train Employees on Back up Best Practices: Employees should know where to back up critical data and know what types of data need to be backed up.

What DOE SBIR/STTR CS Self-Assessment Requirements are being met?

2.B - Minimum Password Strength: The small business should create and use complex passwords that are harder for threat actors to guess or crack.

2.H - Phishing-Resistant Multi-Factor Authentication (MFA): The small business should include additional layer(s) of security to protect assets accounts whose credentials have been compromised.

What is required to implement the CPGs?

To fully implement these CPGs, applicants/awardees should develop, document, and implement processes for creating unique, complex passwords and enforcing MFA. The processes should include specific requirements for password complexity and the use of MFA.

Suggestions for Implementing Minimum Password Strength and MFA:

1. Below are some suggested steps for applicants/awardees to follow to learn more creating strong, unique passwords and implementing MFA:

    a. Training on Password Strength and MFA: Log into the and review training titled, 'Creating Strong Passwords & Two-Factor Authentication' to learn how to create strong passwords.

        i. Another helpful training video the 'Beyond Simple Passwords: Strong Passwords Checklist' can be found on the GCA Toolkit.

        ii. Use Tools to Identify Password Vulnerabilities: The GCA Toolkit also offers a tool to help identify password-related vulnerabilities and check if passwords have been compromised. Beyond Simple Passwords - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

    b. Enforce Complex Password Rules: Many platforms, such as, Google Workspace, Microsoft 365 and AWS allow administrators to set password polices for user accounts at no additional costs. The polices should enforce rules on minimum password length, complexity requirements and password expiration settings.

        i. Use Free and Open Source Password Policy Tools: This is a technical task and may require expertise of a CS/IT professional. Small businesses can use tools like OpenLDAP or FreeIPA to enforce password complexity requirements. For Microsoft users, the local group policy may be used to enforce password polices.

        ii. Ensure the policy addresses how often the user must change passwords. This should be a feature found in the administrative settings of most platforms. This provides an extra layer of protection.

        iii. Small businesses are encouraged to review the NIST Password Guidelines when developing the password policies. Strength of Passwords (nist.gov)

    c. Document the Process for Minimum Password Strength: When documenting your minimum password strength process, consider the following factors:

        i. Password Requirements: Document the requirement for unique passwords for all accounts, including specific criteria for complex passwords (e.g., combination of uppercase and lowercase letters, numbers, and symbols).

        ii. Password Enforcement: Ensure password requirements are documented, maintained, and enforced for all employees. Systems can be configured to ensure passwords meet these criteria.

        iii. Password Storage: Implement processes to ensure passwords are not written down or stored insecurely.

        iv. Password Length: At a minimum, use an 8-character password for accounts with MFA. For accounts without MFA, use a 14-character password. Without

MFA, longer passwords are preferred because they are harder to crack, offering more possible combinations and making them less vulnerable to brute force attacks. (Source: Critical Security Controls v8-5.2).

v. Use of Passphrases to Build Passwords: Passphrases are random words combined to make it easier for the user to remember and meet password length requirement.

2. More suggested training on MFA Implementation:

   a. For MFA training, applicants and awardees should visit the Small Business Cybersecurity Corner | NIST and select 'Multi-Factor Authentication' on the left side of the web page to learn more about MFA.

   b. Additional Training on Phishing and Malware Protection: Applicants and awardees should also view the Protect Against Phishing and Malware training on the GCA Learning Portal.

      i. Download the Phishing Red Flags Cheat Sheet to learn how to identify email phishing attacks. This information can also help with developing processes/policies for enforcing MFA and using unique, complex passwords.

   c. Implementing MFA:

      i. Ensure Systems Are Updated: Before implementing MFA, ensure vulnerability scans are up to date and that your systems are backed up to avoid data loss during configuration.

      ii. Google and Microsoft users have built in MFA that can be enabled for free in the security setup. In addition, Authy is another option that can be used to implement two factor authentication, as well as backup and sync features. This could be useful for small businesses with distributed teams.

   d. Enforce MFA for Critical Assets: To effectively protect critical assets, the small business must decide the level of security needed if credentials are compromised.

      i. Visit the GCA Cybersecurity Toolkit: Beyond Simple Passwords for additional MFA resources.

      ii. Download and implement MFA tools based on your operating system.

      iii. Ensure MFA is implemented on all administrative access accounts and business assets, whether managed in-house or through a third-party provider.

   e. Enable MFA through Password Managers:

      i. Using Password Managers, such as Bitwarden, LastPass, etc. to implement MFA can be a free or a low-cost option for small businesses to MFA capabilities. Allowing user to authenticate with time based one-time

password (TOTP). This also allow for small businesses to manage MFA codes directly within the password manager.

f. Train Employees on Setting-Up and Using MFA: To ensure employees understand the process, training should be developed and part of the small business CS Basic Training Plan.

What is the DOE SBIR/STTR CS Self-Assessment Requirement?

2.W - No Exploitable Services On The Internet: The small business should identify and monitor all assets, especially public-facing assets, and ensure unauthorized users cannot gain an initial system foothold by exploiting known weaknesses.

2.G – Detection of Unsuccessful Login Attempts: The small business should protect its assets from automated, credential-based attacks.

What is required to implement the CPG?

To fully implement 2.W No Exploitable Services on the Internet (means patching vulnerabilities in public-facing systems), applicants/awardees must develop, document, and implement processes to detect and monitor assets (especially public-facing ones) to prevent unauthorized users from accessing critical assets.

To fully implement 2.G Detection of Unsuccessful Login Attempts, processes should be developed, documented, and implemented to protect critical assets from automated, credential-based attacks.

Below are suggestions to help applicants and awardees detect and monitor assets, prevent unauthorized access to critical assets, and implement these CPGs:

1. Most Cloud providers, such as AWS, Microsoft Azure, and Google Cloud, offer managed security features that include firewalls, distributed denial-of-service (DDoS) protection and automatic updates. These features provide high levels of protection for web services and assists small businesses with the task of providing internal security management. Here are some things to consider when enabling the security features:

    a. To prevent unauthorized access to critical assets, ensure only essential services for business operations are used on servers and applications.

    b. Properly configure firewalls to assist with blocking internal services from public access.

    c. Implement Web Application Firewalls (WAF). Usually this is a free (built-in) feature or low-cost service for small business to implement to protect against SQL injection, cross-site scripting (XSS), etc.

2. Understand Exploitable Vulnerabilities: Applicants and awardees should familiarize themselves with vulnerabilities that threat actors can easily exploit. Review Weak Security Controls and Practices Routinely Exploited for Initial Access | CISA to learn about weak controls, poor configurations and bad security practices that leave systems vulnerable.

3. Monitor and Detect Assets: Small businesses should have processes in place to detect and monitor their assets, particularly public-facing ones. These efforts should be part of the access control management, asset inventory, and continuous monitoring processes.
    a. Review the NIST CS Framework v2.0 Small Business Quick Start Guide to learn about the 'Detect' function, which helps businesses find and analyze potential cybersecurity attacks and compromises.
        i. Review: Shields Up: Guidance for Organizations | CISA and develop a plan and processes for quickly detecting and responding to potential intrusions.
        ii. Steps on how to develop an asset detection process can be found in the NIST CSF 2.0 Implementation Examples implementation examples under ID.RA.01.
        iii. Steps on how to develop a continuous monitoring process can also be found on the NIST CSF 2.0 Implementation Examples under DE.CM-06/09 and DE.CM-02.
    b. Review NIST Small Business CS Corner: Guidance by Topic | NIST. On the left side of the web page, select topics: 'Securing Data & Devices and Securing Network Connections' and review to determine appropriate security levels for their devices and best practices.
    c. Reference the CISA Known Exploited Vulnerabilities (KEV) Catalog: This catalog provides information on known vulnerabilities, such as security flaws and misconfigurations. Small businesses can use it to identify and temporarily remediate vulnerabilities they may have.

More suggestions for Small Businesses to Protect Against Exploitable Services on the Internet:

1. Conduct Regular Vulnerability Scans and Penetration Tests: Regularly scan public-facing assets and perform penetration tests to detect exploitable vulnerabilities in systems, applications, and networks. Address identified vulnerabilities promptly.
    a. Use tools like OpenVAS or Nessus to conduct vulnerability assessments.
    b. Patch any known vulnerabilities and misconfigurations as soon as possible.
2. Close Unused or Open Ports: Unused or open ports can be exploited by attackers to gain access to your systems. Regularly check all open ports and ensure only necessary services are running. Use port blockers to secure unused ports.
    a. Use a tool like Port Checker - Check Open Ports Online to check for open ports.
    b. Close any unused ports and disable unnecessary services.
3. Implement Firewalls and Network Segmentation: Use firewalls to protect your network by controlling incoming and outgoing traffic based on predefined security rules. Network segmentation can isolate critical assets from less secure parts of your network, limiting potential damage from an attack.

    a. Configure firewalls with an “implicit deny” rule to block unauthorized access.

    b. Use network segmentation to separate sensitive data and services from general network traffic.

4. Use Secure Remote Access (VPN): Remote access to your network should be protected by using a Virtual Private Network (VPN).

    a. A VPN encrypts the connection and ensures that remote access is secure from eavesdropping and unauthorized access.

        1. Applicants and awardees are encouraged to review Secure Remote Access | Federal Trade Commission (ftc.gov) to learn more about how to implement secure remote access

        2. If applicants/awardees have IT/CS experience and would like to implement VPN then visit the GCA CS Toolkit. Follow instructions and implement ProtonVPN. Here is the link: All Tools - Small Business - GCA Cybersecurity Toolkit | Tools and Resources to Improve Your Cyber Defenses (gcatoolkit.org)

Suggestions for Small Businesses to Detect Unsuccessful Login Attempts:

1. Implement Log Management and Monitoring: Develop a log management process to monitor unsuccessful login attempts. Automated systems should alert administrators if repeated login failures occur, which can indicate a brute-force attack.

    a. Use tools like Splunk or Graylog to collect and analyze logs.

    b. Set up alerts for suspicious login patterns, such as multiple failed login attempts.

2. Strengthen Credential Management: Credentials such as passwords, certificates, and tokens should be protected by strong policies and centralized management tools. Use a credential management tool to enforce password requirements, monitor the use of credentials, and identify any unauthorized access attempts.

    a. Develop a strong password policy that enforces complex passwords and regular password changes.

    b. Use a tool like LastPass or Dashlane to manage credentials centrally.

3. Use Multi-Factor Authentication (MFA): Implement MFA to provide an additional layer of protection. Even if credentials are compromised, MFA will require a second form of verification, making unauthorized access more difficult.

    a. Enable MFA for all user accounts, especially those with access to critical systems.

    b. Use authenticator apps like Google Authenticator or Authy for MFA rather than SMS-based methods.

4. Monitor and Limit Login Attempts: Configure systems to lock accounts after a certain number of failed login attempts to protect against brute-force attacks. Implementing "rate limiting" can also help by slowing down repeated login attempts from the same source.
    a. Set up account lockout policies after a defined number of unsuccessful attempts.
    b. Implement rate limiting on login systems to delay repeated attempts.
5. Review Firewall Access Control Lists: Ensure that access control lists (ACLs) for routers and firewalls are configured correctly to prevent unauthorized access attempts. Implement an "implicit deny" rule so that any connection not explicitly authorized is denied by default.
6. Regularly review and update ACLs. Implement an "implicit deny" rule on all access points to critical systems. Small businesses can effectively protect against exploitable services on the internet and detect unsuccessful login attempts by implementing firewalls, using strong credential management practices, and regularly monitoring access logs (as mentioned above). These are essential steps in maintaining cybersecurity and preventing unauthorized access to critical assets.
7. Related Training: Don't Let Cyber Criminals Steal Your Connections: Securing Internet-Accessible Systems (youtube.com) and Securing Internet-Accessible Systems (usalearning.gov)

What is the DOE SBIR/STTR CS Self-Assessment Requirement?

2.K - Strong and Agile Encryption: The small business should deploy effective encryption to maintain confidentiality and integrity of sensitive data being processed, in transit or at rest.

What is required to implement the CPG?

To fully implement strong and agile encryption, applicants and awardees should develop and implement a process for encrypting data while it is being processed, in transit, or at rest on assets, particularly critical assets. Below are suggestions on how to implement strong and agile encryption.

1. Conduct a Vulnerability Scan Before Implementing Encryption: Before encrypting devices or data, it's essential to ensure that there are no existing vulnerabilities. Use tools to run scans and make sure vulnerabilities are patched. For small businesses, free tools like those offered by CISA or the GCA Cybersecurity Toolkit can be used to conduct vulnerability scans.
2. Keep in mind, Cloud platforms like AWS, Google Cloud and Microsoft Azure offer built-in encryption for data at rest and in transit. These platforms provide encryption as part of their subscription services usually at no additional costs. In additional these platforms may provide key management services (KMS)that can simply key generation, storage and management which can be helpful for small businesses that do not have a dedicated security team.
3. Leverage Built-in Encryption Features: Most modern operating systems like Windows, macOS, iOS, and Android come with built-in encryption tools. For example: Windows

BitLocker: Provides full disk encryption (FDE), macOS FileVault: Encrypts all files on your Mac's startup disk, and Android & iOS: Both provide encryption by default when the device is locked. Small businesses can save time and resources by using these built-in encryptions. However, ensure that these tools are enabled and configured correctly.

4. Use Strong Encryption Standards Implement industry-standard encryption protocols like AES (Advanced Encryption Standard) with 256-bit encryption, which is considered the gold standard for securing data at rest and in transit. AES is widely adopted standard that balances performance with strong encryption. Many commercial and open-source encryption tools support AES.
5. For communication encryption (such as email), use TLS (Transport Layer Security) and STARTTLS for secure email transmission. TLS should be implemented for secure web communications. This is essential for websites and apps to ensure secure data transfers.
6. Data in Transit (Remote Users): Use Virtual Private Networks (VPNs) to secure remote access which is crucial for distributed users/teams. NordVPN Temas or Perimeter 81 provides cost effective and scalable options to assist small businesses. Also end to end messaging tools like Signal or WhatsApp are also low-cost options to secure messaging.
7. Data at Rest/Transit: For secure file storage and sharing, a suggestion is to use services, such as, Dropbox Business and Google Workspace to secure data. Also, adding Boxryptor tool is an extra layer of protection that small businesses can use to secure data.
8. Multi-Layered Security Approach Encryption is an essential component for this CPG, but not a standalone solution. Implement additional layers of security to strengthen the overall defense, including:
    i. Phishing-resistant multi-factor authentication (MFA) for access control.
    ii. Firewall rules and access control lists (ACLs) to restrict access to encrypted systems.
    iii. Regular Encryption Key Management Ensure you have a proper process for managing encryption keys. Regularly rotate encryption keys and store them in a secure key management system. If encryption keys are compromised, the security of encrypted data is also compromised.
    iv. Ongoing Monitoring and Auditing Establish processes for monitoring encryption health and ensure that encryption is always enabled where it is required. Periodic auditing helps identify if any encryption mechanisms have been disabled or misconfigured.
9. Develop, document, maintain and enforce the process associated with the procedures mentioned above.

Related Training: Related Training Resources: Securing Network Infrastructure Devices | CISA

What is the DOE SBIR/STTR CS Self-Assessment Requirement?

2.M - Email Security: The small business should reduce risk from common email-based threats, such as spoofing, phishing, and interception.

What is required to implement the CPG?

To fully implement 2.M Email Security, small businesses should develop, document, and implement processes for applying security measures to protect emails from common email-based threats. These processes should focus on protecting against spoofing, phishing, and the interception of sensitive information.

Below is suggested training and information on how to implement email security:

1. Train employees to recognize email threats: Ensure that I Basic Cybersecurity Training is implemented within your workforce. This training should focus on recognizing and responding to email-based attacks like phishing and spoofing. Regular phishing simulations can help reinforce this knowledge.
2. Log into the Global Cyber Alliance Learning Portal: https://edu.globalcyberalliance.org and review the training called, 'Protect Against Email Spoofs & Phishing' to learn more about securing your emails.
    a. Download and complete the 'Protect Your Email & Reputation: Email Security Checklist'
        i. Start with DMARC, SPF, and DKIM: Setting up DMARC, SPF, and DKIM is crucial to prevent email spoofing and ensure the integrity of your emails. These protocols authenticate the legitimacy of emails sent from your domain and help block phishing attempts. Action Steps:
            1. Use the GCA DMARC Setup Guide to configure these protections.
            2. Regularly monitor your DMARC reports through tools like Valimail Monitor to understand where email-based attacks may be targeting your domain.
            3. Use TLS Encryption for Email in Transit: Ensure that emails are encrypted in transit by configuring STARTTLS or TLS for all mail servers. For businesses that use email services from providers like Gmail or Microsoft 365, TLS encryption is typically enabled by default, but it should be verified.
            4. For custom email servers, use Let's Encrypt (Let's Encrypt (org)to obtain free TLS certificates.
                a. Ensure that email clients are configured to require encryptions for all outgoing emails.
                b. Set up Domain-based Message Authentication, Reporting, and Conformance (DMARC) to protect your small business's domain from spoofing. DMARC provides reports and

enforces email authentication policies to reject or quarantine unauthorized

3.

4. Additional email security features that can be enabled for Yahoo, Google and Microsoft users are listed below:

    a. Yahoo offers 2-Step Security Key for email accounts to add an extra layer of protection.

    b. Google offers 2-Step Verification for Gmail accounts. Visit the Gmail Help Center to learn more about their security and privacy features.

    c. Microsoft 365 (MS 365) offers email encryption through Outlook.

        i. To enable this, go to the File tab, choose Options > Trust Center > Trust Center Settings. Under Email Security, select the Encrypt contents and attachments for outgoing messages checkbox.

        ii. Additional settings, such as choosing a specific certificate, can be managed under Settings.

5. Related Training: Don't Let Cyber Criminals Cash In – Preventing Business Email Compromise (youtube.com) Understanding Web and Email Server Security (usalearning.gov)

What is the DOE SBIR/STTR CS Self-Assessment Requirement?

2.S Incident Response (IR) Plans: The small business should develop, document, maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.

4.A - Incident Reporting: The small business should have security incident reporting procedures to contact an internal incident response team and/or senior management. In addition, the small business should have available the contact information of CISA, FBI, or local police for assistance with security incidents or to understand the broader scope of a cyberattack.

What is required to implement the CPGs?

To fully implement the Incident Response Plan and Reporting, a process should be developed, tested, maintained and implemented to ensure the small business is prepared to handle security incidents and report them to the appropriate authorities.

The DHS CRR Supplemental Resource Guide, Incident Management is suggested along with this implementation guidance. Note: Check with your current IT service provider, as coverage may already be available to satisfy this CPG requirement.

1. Develop a Clear IR Plan: Ensure that your IR Plan outlines all necessary steps (processes) for detecting and responding to incidents, including defining roles, responsibilities, and communication protocols. Enforce and regularly update the plan to account for new threats

or changes in your business, particularly concerning critical or high-value assets.
Suggestions to Implement the Incident Response (IR) Plan:

a. Identify High-Value/Critical Assets: Ensure that critical or high-value assets, as listed in your asset inventory, are identified. These assets are most vulnerable and require the highest level of protection.

b. Identify Threat Scenarios: Outline threat scenarios that could severely impact critical or high-value assets if compromised during a security incident.

c. Define Security Incidents: Establish, document, enforce and disseminate the criteria for what constitutes a reportable security incident, including the type of incident, the criteria for reporting, and acceptable reporting timelines. This information should be used to develop Incident Reporting process (see below).

d. Assign Key Roles and Responsibilities: Establish key stakeholder roles, responsibilities, and communication channels for reporting security incidents. This should include documentation of mitigation measures, identified vulnerabilities, and risks accepted.

e. e. Define Communication and Escalation Channels: Establish communication channels to share information related to security incidents, including mitigation measures, new vulnerabilities, and accepted risks. Ensure this information is tracked, documented and used in the Incident Reporting process. Establish Incident Response Objectives: Develop an IR Plan that includes predefined steps for detecting, analyzing, containing, eradicating, recovering from, and reporting security incidents.

f. Test the IR Plan: Verify that the IR Plan meets security requirements to protect critical or high-value assets through regular testing.

g. Conduct Regular Training: Regularly train employees and conduct drills to ensure that they are familiar with the IR Plan, understand their roles, and can respond effectively to incidents.

h. Use Incident Reporting Forms: Develop a standard form to document security incidents (date, time, location, individuals involved, description, actions taken, etc.). Ensure this form is available to all personnel and used during the IR reporting process (see below for more information on IR Reporting).

i. Include Remote Work Provisions: With an increase in teleworking, ensure that your IR Plan accounts for incidents that occur when employees are working remotely. Make sure remote employees know how to report incidents securely.

2. Incorporate Incident Reporting: Incident reporting should be a formalized part of your IR Plan. Ensure personnel know how to report incidents, who to contact, and what details are necessary for incident documentation. Suggestions on how to Implement Incident Response (IR) Reporting:

a. To develop Incident Reporting the small business should utilize its IR Plan to develop and enforce Incident Response process that should be updated yearly or as needed, also to include the following, but not limited to:

    i. Assign Key Personnel: Identify and assign roles to key internal and external stakeholders responsible for reporting incidents to Incident Response personnel. This includes contact information for CISA, the FBI, or local police.

        a. A list of key stakeholders within the business, such as, the Cybersecurity Lead and the SBIR/STTR Small Business Owner should be primary contacts for incident reporting as well.

    ii. Address Teleworking and Remote Access: Include provisions for personnel working remotely or telecommuting in the incident reporting process.

    iii. Disseminate the Process to Stakeholders: Ensure that the IR Reporting Process/Plan is distributed to all stakeholders.

    iv. Report security incidents to local police (if needed);

        a. Maintain updated contact information.

        b. If on site presence of local police is required, then ensure process for access/entry to the work site is established.

    v. Report Cyber Incidents to CISA:

        a. Review the CISA site: Voluntary Cyber Incident Reporting | CISA to learn more about CISA's recommendations for 'why, when, what and how' to report cyber incidents.

        b. Use the CISA Services Portal: IRF Index - IRF (cisa.gov) to report incidents, if needed.

        c. The portal allows users to save and update reports, share them with colleagues, and engage in informal discussions with CISA regarding incidents.

        d. Maintain updated contact information.

    vi. Report Cyber Incidents to the FBI:

        a. Use the FBI Internet Crime Complaint Center (IC3) to report incidents, if needed.

        b. Maintain updated contact information.

    vii. Test the Process: Regularly test the IR Reporting Process/Plan to verify that it meets the business's reporting objectives.

    viii. Ensure that the IR Reporting Process/Plan is integrate into the IR Plan

3. Related Training: CISA Incident Response Playbooks:

CISA Cyber security Incident Response Playbooks - Episode 1 - Overview - YouTube

4 Wix Features You Gotta Know (youtube.com)

CISA Cyber security Incident Response Playbooks - Episode 2 - Preparation Phase (youtube.com)

CISA Cyber security Incident Response Playbooks - Episode 3 - Detection Phase (youtube.com)

CISA Cyber security Incident Response Playbooks - Episode 4 - Containment (youtube.com)

CISA Cyber security Incident Response Playbooks - Episode 5 - Eradication and Recovery (youtube.com)

CISA Cybersecurity Incident Response Playbooks - Episode 6 - Post-Incident Activity (youtube.com)

CISA Cyber security Incident Response Playbooks - Episode 7 - Coordination (youtube.com)

CISA Cyber security Incident Response Playbooks - Episode 8 - FTK and CISA (youtube.com)