U. S. Senate
Sergeant at Arms

Standard Operating Procedures
For
Cybersecurity

October 2021

Table of Contents

Document Revision History

Version	Description	Date
3.0	Reorganized the document to place policy related content in sections 1,2, and 3 of this document and contractor requirements in sections 14 and 15 including content updates incorporating previously separate cybersecurity related contractor requirements documents. Also added breach notification, vulnerability remediation timeframe, and cloud service cybersecurity contractor requirements to section 14, and removed references to Senate Mainframe system which was retired from service in 2021.	10/05/2021

1 U.S. SENATE INFORMATION SYSTEMS SECURITY POLICY FOR SENATE UNCLASSIFIED SYSTEMS AND NETWORKS

As a critical part of our nation's leadership, the United States Senate (the Senate) processes and develops information vital to our nation's well-being. The Senate information technology environment is a valuable asset in carrying out legislative responsibilities and daily functions. Senate members, staff, and support elements require timely access to reliable information processing for both routine operations and major decisions. The Senate has a responsibility to protect its information from the threat of unauthorized access, modification, destruction, or disclosure, and to protect its information assets from loss or misuse.

The Senate is a large, diverse organization whose systems include hundreds of local area networks (LANs) on Capitol Hill and at state offices, mainframe computer services, and networked resources both within the Senate and with other Legislative Branch organizations. The Senate also relies on access to commercial and public (Internet) information services. Interconnectivity provides Senate users with remarkable resources and capabilities, yet it also significantly increases the risks to Senate systems. In a networked environment, consideration must be given to the risks of such connections.

Security of a network is determined by the security afforded each component level. As a result, a local risk management decision becomes a global risk management decision since the total is only as protected as its weakest link. In order to manage the risks associated with its networked environment, organizations must balance their information technology needs with the need to provide due care and diligence to protect not only all Senate information and systems, but also those systems to which Senate systems are linked.

The Senate's Information Systems Security goals are:

- to assure adequate levels of protection, confidentiality and integrity of Senate systems and networks;
- to prevent or detect and counter threats to Senate information and systems; and
- to ensure that Senate information and information processing assets are available when needed.

These goals include the following:

- information is protected against unauthorized access;
- information is protected against unauthorized modification;
- information maintains its integrity;
- information will be available when needed;

- systems are protected against unauthorized modification;
- systems are not subject to denial of service;
- systems are not subject to accidental or malicious destruction;
- systems cannot be used as a "pass through" for unauthorized access to other networks/systems;
- systems maintain the integrity of Senate information and the system security features implemented; and
- contingency operations will meet the needs of the Senate.

The Senate handles sensitive information and operates critical information technology systems, both of which require protection. Senate information may be sensitive, proprietary, or classified.

- The integrity of Senate information and systems is critical to maintaining public confidence.
- Instructions/policies regarding Senate classified systems are issued by the office of Senate Security.

This Information Systems Security policy applies to all Senate unclassified systems utilizing information technology, to include:

- automated information systems;
- networks;
- telephone switching equipment and voice mail systems;
- video teleconferencing;
- physical alarm systems;
- physical access systems (i.e., badge readers);
- web and mobile applications;
- communication software;
- computerized facsimile; and
- other computer-based systems and software.

Within the Senate, the Sergeant at Arms Chief Information Officer is responsible for assuring adequate levels of protection for those information technology systems which it operates/maintains on behalf of the Senate. Such systems include the Senate Network, Mainframe, physical and virtual servers, storage, etc. Each individual Senate office is responsible for assuring the protection of those information technology systems which it owns/operates.

This Information Systems Security policy applies to Senate and non-Senate personnel (i.e., vendors, contractors) operating, maintaining or using Senate information processing resources including those provided as cloud services.

The SAA Cybersecurity Department is the focal point for information system security issues which affect US Senate systems and operations. The Cybersecurity Department will:

- maintain a Senate-wide information security incident response capability to support timely notification and response to threats to Senate information technology systems;
- collect pertinent information on information technology systems, their vulnerabilities and threats, and disseminate it, as appropriate, to Senate elements; and
- work with appropriate offices to address information security problems that may affect Senate systems.

At the request of individual Senate offices, the Cybersecurity Department will also provide:

- guidelines presenting physical, personnel, communications, hardware, software, and procedural security measures to protect information technology systems from inadvertent or deliberate compromise, damage or destruction;
- advice and assistance in helping Senate offices understand, establish, and implement information security measures;
- information security services (i.e., technical assistance, risk assessments, etc.); and
- information security education and awareness presentations.

2 SERGEANT AT ARMS CYBERSECURITY POLICY

Information in all its forms and through its life cycle will be protected from unauthorized modification, destruction, disclosure, or denial, whether accidental or intentional. The cost of such protection will be consistent with the sensitivity and value of the information to the United States Senate. This protection includes the peripherals, hardware, and software used to process, store, and transmit the information.

Each Sergeant at Arms (SAA) department or office is responsible for determining the sensitivity of the data created and/or processed in the organization and establishing and/or defining appropriate controls and acceptable levels of risks. Under certain circumstances, it may be necessary for the SAA department or office to access a Senate-issued computer to an employee, contractor, or temporary help to recover documents. For this reason, the Office of the Sergeant at Arms reserves the right to access all computer files stored on SAA department or office workstations at any time.

Information stored on department or office computers is the property of the Senate and is not private. Employees of the SAA, contractors, or temporary help on assignment to the United States Senate may not make copies of any software licensed to the Senate or to the SAA and

remove it from the department or office. Employees, contractors, or temporary help on assignment to the United States Senate are also prohibited from using unlicensed software on individual computers or LAN's.

The Sergeant at Arms has established the Cybersecurity Department which is responsible for ensuring that appropriate organizational security procedures and standards are developed to support the cybersecurity policy. The Cybersecurity Department is responsible for coordinating the implementation of information security measures within all SAA departments and offices, and providing management assurance that the organization is in compliance with policy, legislative, and contractual requirements regarding cybersecurity.

2.1 Compliance

Non-compliance with this policy may lead to disciplinary action by the SAA, including revocation of computer user privileges, admonishment, reprimand, suspension, or termination of employment. Under certain circumstances, unauthorized access to or modification, disclosure, or destruction of Senate information may give rise to civil and/or legal activity. Any computer systems that do not adhere to Senate or SAA cybersecurity policies, or for which no specific Senate or SAA cybersecurity policies are published may be refused access to the Senate data network and may be deemed inappropriate for storing or accessing Senate information.

3 OFFICE OF THE CHIEF INFORMATION OFFICER CYBERSECURITY POLICY

3.1 Purpose

Under the U. S. Senate Information Security Policy, the SAA is responsible for assuring protection for information technology systems operated and maintained on behalf of the Senate. It is the policy of the Chief Information Officer (CIO) to take appropriate measures to assure adequate levels of security, confidentiality, and integrity of U. S. Senate information and information technology resources under its custodianship.

3.2 Scope

This policy applies to all U. S. Senate information technology resources and to all employees, contractors and any other individuals who access, process, or have custody of Senate information using the SAA's services and facilities.

3.3 Objectives

The objectives of this policy include but are not limited to the following:

- provide a high level of security and integrity for information technology resources and data;

- prevent any compromise of the integrity, availability, or confidentiality of the data or the systems that process and store data;
- safeguard proprietary, personal, privileged, or otherwise sensitive data entrusted to the SAA;
- ensure individual accountability; and
- ensure the ability to survive hazards and maintain continuity of operations consistent with the criticality of information requirements.

3.4 Responsibilities

The CIO is responsible for providing enforcement of and top management support for the Cybersecurity Policy.

The SAA Directors, Managers, and Supervisors are responsible for developing security requirements and monitoring proper safeguard practices relative to their functional areas. This includes strict adherence to all protection and control criteria specified by an information owner for data, applications, and services under the SAA's custodial control. They shall maintain effective overall controls to prevent damage or destruction that might adversely affect an information owner's operational schedule.

All SAA employees and contractors are required to protect assets assigned to them, to implement and enforce the established security practices and procedures, and to notify SAA/CIO management or the Senate COR, if applicable, of security violations and problems.

Senate offices are responsible for establishing, publishing, and implementing safeguards relative to maintaining the security of their office systems and for the information maintained on those systems.

Owners and/or originators of applications and services that operate on the SAA's platforms are responsible for specifying the security requirements usage controls, and access controls for those applications and services.

Every originator, custodian and/or user of Senate information must ensure that the data under his or her direction and/or control is properly identified and safeguarded according to its sensitivity, proprietary nature, and criticality.

Individuals with access to the SAA facilities are allowed only the use of information technology resources and information for which they are authorized. Such authorization must be obtained from the individual's supervisor or the Senate COR, whichever is applicable. They must adhere to

the specific security measures and controls that have been established for those resources and information.

3.5 Standard

The SAA CIO Cybersecurity Policy and Standard Operating Procedures (SOPs) will serve as the minimum acceptable requirements for data security practices to be applied by management and employees. In addition, these SOPs will be a basis for compliance, monitoring, and review.

3.6 Enforcement

Violations of standards, procedures, or guidelines established in support of this policy will be brought to the attention of the CIO for appropriate action. Failure to follow established security policies and procedures may result in admonishment, reprimand, loss of access privileges, suspension, termination of employment, and/or liability for damages depending on the severity of the violation.

4 NON-DISCLOSURE OF SENSITIVE INFORMATION

Employees, contractors on assignment to the Senate, and all others granted access to SAA facilities and information resources may not disclose, assist in, or facilitate the disclosure of sensitive information by any means--verbally, materially, electronically, or otherwise--to any person or agency not entitled to receive it. Sensitive information includes the following:

- Senate Office Data (information of which SAA Departments have been given custody by any Senate office or information which the SAA maintains for any Senate office);
- Computer Software and Supporting Documentation (licensed commercial software and systems developed in-house); and
- Personally Identifiable Information (PII) (home addresses, home telephone numbers, social security numbers, date of birth, employment history, salary, credit or any other financial or personal information relating to Senate staff).

In accordance with Rule XI of the Standing Rules of the Senate, Senate property, records or documents may not be released or removed without proper authorization, and such property or information may not be used for personal reasons.

Violations of this policy will be brought to the attention of management for appropriate action, which could include termination of employment and/or liability for damages.

5 ACCESS TO SENATE OFFICE INFORMATION

5.1 Senate Office Systems

Senate offices are responsible for establishing, publishing and implementing safeguards relative to maintaining the security of their office systems and for the information maintained on those systems. They control access to their own computer systems both locally and remotely. SAA technical support staff (including support contractors) may at times require access to these systems, but the office controls the extent and degree of access. Each office must weigh for itself the risks of providing access to support staff against the necessity of sustaining efficient, reliable, and secure system operations.

In all cases, SAA support staff may access an office system only when they have been granted specific permission by the office. The permission is normally granted by the office providing the support staff member with a logon ID and password combination to allow access. Once logged onto a Senate office system, support staff may be given privileged administrator capabilities so they can resolve critical problems. The Office is responsible for monitoring all work performed under these circumstances and ensuring that access privileges are not misused.

Remote access increases risk but may be necessary at times when problems cannot be resolved over the phone and someone cannot quickly or easily be dispatched to an Office. System unavailability for the length of time needed for a technician to travel to the Office, log on the system, diagnose and correct the problem may not be acceptable for some Offices. In these instances, remote access by SAA support staff can represent an acceptable risk for timely resolution of an acute problem. Usage of a one-time password can reduce the risk.

Offices are advised to establish a special account that is activated only when remote support requiring high-level privileges is needed. The password should be changed after each support effort so that access is allowed only for a limited period. Offices are cautioned to closely monitor system activity at times when this account is used. An Office can validate the identity of anyone requesting remote access over the telephone by asking for a number to call the person back. The Office can verify the number before calling back and providing access.

5.2 Senate Office Information on SAA Resources

Senate office data transmitted over networks or stored on central computer platforms, including cloud platforms, provided by the SAA is never monitored for content unless specifically requested in writing by the Senator or Office authorized personnel and authorized by the SAA. In that instance, monitoring is performed on the requesting Office's data as authorized and only for a limited length of time. All monitoring information is turned over to the requesting office. No monitoring data is retained on file by the SAA.

Offices maintaining information on platforms operated by the SAA are responsible for specifying the security requirements, usage and access controls for their information. For these situations, it may be necessary for SAA support staff to access Senate Office data to address a problem. In all such cases, consent from the Office to access this information must be obtained first.

SAA staff assisting Senate offices with managing their information on central platforms should:

- access Senate Office data only to the extent necessary to perform the work needed to assist the Office;
- never reproduce Office data unless specifically directed to do so by the Office;
- never disclose Office information to third parties without written consent of the Office; and
- return all data (including copies) to the Office.

  If an emergency requires access of Senate Office information to maintain the integrity or availability of the Senate technology infrastructure, the Office will be advised that its assistance is required to address the situation.

In the course of their regular duties, SAA support staff may discover evidence of violation of Senate or SAA security policies. Violations should be reported to the SAA and the responsible Senate office. Staff requested to participate in an investigation will be approved by the SAA and the Senate Office.

6 PROJECT MANAGEMENT

Security and controls must be designed into the services and products provided by SAA departments. Project Managers are responsible for determining measures needed to meet a project's operational purpose in a practical, usable, cost-effective fashion without sacrificing security.

A Project Manager should determine the following:

- who owns information;
- who is responsible for the integrity of information and other resources;
- who is to allow or deny access to information and on whose authority;
- who is responsible for detecting security violations or compromises;
- who conducts security reviews; and
- what are the security responsibilities of individual users and how are these communicated.

Security measures are most effective when addressed in the design phase. Potential risks should be identified and evaluated, and cost-effective safeguards selected to provide prudent levels of protection without sacrificing productivity.

It is important to note that absolute security is not achievable. In some cases, it may be reasonable for management to decide to accept some risk rather than expend resources mitigating such risk. The cost of having enough levels of security and availability must be balanced with efficiency and usability. Controls should not be excessively cumbersome to the users of the product or service.

The ability to recover from a disruption of services is also a major consideration. A determination must be made as to the level of effort that is justified to satisfy requirements for continuous availability.

Security responsibilities in the development and deployment of SAA products and services.

- Apply the Principle of Least Possible Privilege. Limit users to information and transaction authority as spelled out by the information owner.
- Provide for individual accountability. Have the information owner identify significant events that should be recorded and tracked.
- Screen contractor staff and require them to undergo a background check before providing privileged access to Senate resources.
- Remove privileged access when that access is no longer needed. When an employee announces his or her intention to resign, immediately remove all privileges except for those needed to close out assignments.
- Educate all project staff, including contractor staff, on their personal and supervisory security responsibilities.
- Monitor Security. Establish a way to detect unusual events and bring them to the attention of the appropriate party.
- Develop a method to verify that the product or service is functioning as intended. This can also be used as evaluation criteria for security audits.
- Provide a method to recover from troublesome events, whether minor problems or major disruptions. Availability is a question of what outages or loss of service can be tolerated.
- Safeguard all sensitive documentation. This includes documentation that reveals the logic, methodology or procedural aspects of applications or system software. Documentation should be stored in secure areas, and duplicates stored at an off-site location.
- Safeguard all media on which information is represented or stored to a level commensurate with the sensitivity of the information it contains.

- All information on the Senate systems is considered to be sensitive and should be afforded some protection. The information owner should provide guidance regarding the sensitivity level of data. Protect media identified as containing sensitive information from unauthorized access. Keep sensitive reports in a secure location.
- Sanitize highly sensitive data from magnetic media and shred documents containing highly sensitive information when no longer needed.
- Develop controls to prevent misuse of an SAA product or service.
- Assess the security implications on the existing Senate infrastructure prior to introducing any new products or services.

7 SYSTEM ADMINISTRATION

System Administrators are responsible for implementing appropriate security measures on the systems they administer. Each Administrator is expected to establish controls to protect information assets and ensure continuity of system operations. Selected controls should be appropriate for the sensitivity, criticality, and value of the information stored and processed on the system.

The following checklist outlines what is expected of Administrators in applying baseline security measures.

- ✓ Inform users of system security policies, guidelines, and standard operating procedures.
- ✓ Maintain a plan to address disruptions and extensive service interruptions.
- ✓ Physically secure sensitive or critical file servers.
- ✓ Physically secure external modems for remote connections.
- ✓ Use available operating system security features.
- ✓ Apply vigorous password management for privileged accounts.
    - Require a minimum password length of twelve characters
    - Assign unique logon IDs to all users.
- ✓ Eliminate guest and generic IDs.
- ✓ Safeguard the Administrator account.
    - Enroll the account in the Senate Privileged Account Management (PAM) service
    - Select a password with a minimum length of twelve characters.
    - Change the password at least every three months.
    - Use the account only when administrator privileges are needed.
    - Do not use the account when accessing the Internet.
- ✓ Promptly deactivate accounts for terminated or reassigned staff.

- ✓ Use available monitoring and auditing facilities to log security relevant events and review logs daily.
- ✓ Provide only necessary operating system functionality and remove any unneeded programs and services.
- ✓ Monitor electronic mailing lists for news of new operating system vulnerabilities and apply and test relevant security patches promptly.
- ✓ Maintain backups of the current operating system and application configurations.
- ✓ Make frequent backups of critical files on a regularly scheduled basis as defined by the system owner.
- ✓ Store backups in a secure, environmentally protected location at least 100 feet from the file servers. Enterprise Operations Enterprise IT Systems Branch can arrange for storage at the Senate's off-site facility.
- ✓ Use all appropriate Cybersecurity Department specified anti-virus/anti-malware software and update signature files regularly.
- ✓ Maintain records of security problems and violations to help identify patterns and trends that point to new vulnerabilities or the weakening of existing controls.
- ✓ Assess the security implications of any new technology prior to implementation.
- ✓ Establish an Emergency Access Account (EAA). Place the EAA logon ID and password in a sealed envelope marked for emergency use only. Store the envelope in a secure, locked place known to system management. Change the password after use.
- ✓ Notify SAA/CIO Cybersecurity Department at 202 228 2927, option 1, or email csoc@saa.senate.gov of any suspected security breach or violation.

8 COMPUTER USER GUIDELINES

All individuals with access to Senate computers and networks are expected to understand, respect and follow established security policies. They are personally accountable for their actions when using these resources. The following checklist outlines what is expected of everyone using Senate information technology:

8.1 User Responsibilities

- Do not circumvent security mechanisms and procedures established to protect information.
- Use screen saver passwords, anti-virus software, and other available safeguards.
- Use effective password management. Select good passwords and protect them from disclosure.
- Safeguard your Multifactor Authentication (MFA) token and other access devices.
- Protect against introducing viruses or malicious code into any Senate computer.
- Honor copyright and license restrictions.

- Do not attempt to gain unauthorized access to information.
- Use only authorized software on your computer.
- Do not use software, equipment, or communications lines for anything other than authorized use.
- Use electronic mail properly. Do not “snoop” or “spoof.”
- Conform to the published terms of use on all systems and networks.
- Delete sensitive files so that residual data is not retrievable by others.
- Check the credentials of anyone who works on or services your computer.
- Immediately report any security incident involving computers or networks to your System Administrator.
- Complete annual Cybersecurity awareness training.

8.2 Basic Computer Care

- Locate your computer away from sources of heat and direct sunlight. Computer equipment is sensitive to extreme changes in the office environment.
- Keep your computer’s air vents free of obstruction so the system has adequate ventilation.
- Use your surge protector to prevent problems with spikes, surges and dips in the power supply.
- Keep your work area as clean and dust-free as possible. Occasionally wipe the exterior surfaces of the system with a soft, damp cloth.
- Food particles, liquids, ashes, and smoke residue can damage equipment. Avoid eating, drinking and smoking near your computer.
- Do not move computer equipment yourself. You can seriously damage a computer and data stored on its fixed disk by moving it improperly. Contact your System Administrator about relocating equipment.
- Do not open any part of the system. Removing covers can violate manufacturers’ warranties.
- Handle removable storage (e.g. CDs and DVDs) with care. Acquire removable storage boxes from the Stationery Store to protect such storage when not in use.
- Avoid extremes of heat and cold when storing computer media.
- Protect removable storage from dust, cigarette ashes, crumbs, and liquids.

8.3 Securing the Work Area

- Do not provide access or information to strangers.
- Politely challenge and assist people who do not belong in your work area.
- Do not let unauthorized personnel work on or service your computer.
- Examine the credentials of service personnel you do not recognize or are not expecting. Contact your System Administrator immediately if you have any reservations.

- Use the password feature of your screen saver.
- Log off or lock your computer before leaving it unattended.
- Keep removable storage such as thumb drives, CDs, and DVDs in a secure place so they cannot be picked up by visitors.
- Shred or otherwise destroy paper output (computer listings, reports, etc.) that contains sensitive information. Do not discard such output in waste cans where it can be retrieved by others.

8.4 Closing Up at the End of the Day

- Log off and power down your computer.
- Lock up sensitive documents and removable storage containing sensitive data.

8.5 Working Away From the Office

- Maintain good security practices with your laptop or home computer.
- Do not copy office files to your laptop or home computer without authorization.
- Safeguard laptops, mobile devices, and removable storage such as thumb drives, CDs, and DVDs from theft or accidental loss while traveling.
- Only connect to the Senate using Senate approved/issued devices. Office files stored on a home computer can be accessed by other family members and their friends. Take precautions so that they are not copied along with games or other software.
- Do not store office removable storage such as thumb drives, CDs, and DVDs with that for home use.
- Use virus detection software on your home computer or laptop and keep it up to date.
- Transport computer media in proper containers. Magnetic field sources you encounter in transit can erase computer data.
- Never leave a mobile device or removable storage such as thumb drives, CDs, and DVDs in your car or anywhere where it may be exposed to rapid temperature variations or sunlight.

8.6 Selecting Good Passwords

- Select obscure passwords that are easy for you to remember and hard for others to guess.
- Don't use your name, logon ID, birthday, address, telephone, license plate, or social security number.
- Don't use persons, places, or things that can be closely identified with you.
- Don't use any word you can find in a dictionary.
- Do combine upper/lower case letters, numbers, and special characters in your password.

8.7 Protecting Passwords

- Do not share your password or reveal it to others.

- If it is necessary to disclose your password, change it when the need for others to know it is over.
- If you write down your password, lock it up. Do not leave it where it can be easily found.
- Change your password at least every year.

8.8 Computer Viruses

- Use Senate approved virus detection software on your computer.
- Scan all incoming removable media, files, and programs for viruses.
- Keep virus detection software up to date.
- Use only authorized software or software from reputable sources
- Report any virus infection to your System Administrator.

8.9 Imported Software

- Do not import or download software without authorization.
- Import or download software only from official sources.
- Get source code if possible.
- Use data integrity check programs to verify imported software.
- Check out software on a computer not connected to a LAN.
- Never execute programs from an unknown or unreliable source.

8.10 Protecting Against Disaster

- Be sure to back up all critical data.
- Make multiple copies of critical files.
- Keep the back-up copies up to date.
- Store backups in a secure place.
- It is not necessary to backup SAA-provided programs. System Administrators maintain backups of software and of data stored on file servers.
- If you have software that you've installed yourself, make a backup copy before you load it on your computer and write protect that copy. Store the original installation files in a secure location. Scan the files for viruses before making the backup, and do not proceed with the backup if you discover a virus.
- Contact your System Administrator if you are not sure what files you need to back up yourself.

8.11 Deleting Files

- Remember that simply deleting or erasing a file may leave residual data that is still accessible to someone with the proper tools.

- Do not dispose of storage media or release computer equipment for replacement or repair without taking precautions to physically remove sensitive information, including residual data from deleted files.

8.12 Copyrights

- Do not copy licensed software for the purpose of installing it on another computer. Unauthorized reproduction of copyrighted software is against the law. Software installed on your computer is authorized for in-office use only.
- Do not make copies of the documentation provided with Senate-supplied software unless copying is authorized in the license agreement.

8.13 Email Guidelines

- Do not send unnecessary emails.
- Write clear, courteous email messages that reflect well on you and the Senate.
- Consider how your email message may be perceived if it is forwarded to another unintended recipient.
- Do not send an email message while you are angry or upset.
- Be careful with addressing. A simple keying error can result in your message being sent to the wrong individual or distribution list.
- Do not have any expectation of privacy with email unless you encrypt your messages.
- Do not react to inflammatory or unusual mail without checking with the originator to make sure he or she actually sent the message and that it has not been altered. Disguising identity or altering messages on email is not difficult.
- Do not store or execute an attachment from an unknown source.

8.14 Communications

- Do not use an analog line for anything other than its intended purpose.
- Protect your MFA device. Do not lend it to anyone else. Lock up your PIN. Never keep the PIN with your device.

8.15 Internet

- Do not transmit anything over the Internet that requires confidentiality without encrypting it first.
- If you receive an email message that is out of character for the sender, examine the message's header information for evidence of a forgery. The header sent with Internet email messages identifies the sender, the host from which the message was sent, and a list of mail-forwarding hosts through which the message traveled to reach you.

- For sensitive email, use an encryption key to create a digital signature to sign your email message. Signing a message in this way proves the sender is the true originator and that it has not been altered by anyone else.
- Never store any email attachment from an unknown source on your computer
- Never execute any program received in an email attachment from an unknown source
- Disable ActiveX and Java on your Web browser before visiting any site where you are not sure of its authenticity. Hostile applets can delete files, read private data or infect your computer with malicious code.
- Access only known sites that safeguard their postings from tampering.
- Download executable files only from reputable sites.
- Contact your Systems Administrator if you require an application to be installed on your system. Only download business required software from legitimate sites on the Internet and scan them using Anti-Virus prior to installation. Checksums or other provided methods to verify the authenticity of the application can also be used to ensure that the application has not been altered.
- Scan every program obtained from the Internet with an up-to-date virus detection utility. Remember that virus scanners detect only viruses and may not catch other types of destructive code that may be hidden in another program.
- First test any software obtained from the Internet on a system that is not connected to the Senate network to limit any damage in case it does contain destructive code.
- Make sure you access files directly from the official source. Files posted by a secondary source may have been altered. A URL may have been changed so you may not actually be at the page you intended to access. Double check the URL to make sure you are at the correct location.

8.16 Reporting Violations

- Notify your System Administrator of any suspected computer/communications misuse, abuse or security incident.

9 CLASSIFIED NATIONAL SECURITY INFORMATION

Only key members and staff of the U.S. Senate receive, produce, and maintain classified information vital to national security. This is official information which requires protection in the interests of U.S. national security. It may relate to national defense, foreign relations, economic matters, or critical technologies. It is the exclusive property of the U.S. government.

The Office of Senate Security under the Secretary of the Senate ensures that classified information is strictly controlled. Regulations governing its management are outlined in the U. S. Senate Security Manual.

Only staff having a valid security clearance on file at the Office of Senate Security may have access to classified information or systems that process classified information. SAA staff with clearances are expected to be familiar with and abide by the regulations in the U. S. Senate Security Manual. Senate staff may not sign for or directly accept classified documents. Couriers delivering classified material should be directed to the Office of Senate Security (SVC-217).

The Office of Senate Security (202-224-5632) should be called immediately if a document is discovered which appears to be classified or any time a breach involving classified information is suspected.

10 REMOTE NETWORK ACCESS

Remote access to common services on the Senate Network and specifically-authorized LANs are available to those with a valid MFA account and its associated device which may be the authorized user's Senate provided mobile device with a Senate provided software authenticator app or a purpose specific hardware token (MFAT). Supervisors can acquire accounts for themselves and their staff by forwarding a request through TranSAAct.

A MFAT is a security device that automatically displays a randomly generated access code which is used as a password. The Senate provided mobile device or MFAT is typically used with Cisco AnyConnect VPN software to access the Senate VPN.

All MFAT users are expected to:

- safeguard the MFAT and never lend it to anyone else; and
- report a lost or stolen MFAT immediately to IT Support Services Telecom Help Desk (202-224-9611).

While a MFAT is rugged, it is also a delicate instrument. Precautions to be followed include the following:

- do not drop or bend it;
- do not leave it in your car or anywhere else where it may be subjected to extremes of temperature;
- do not subject it to undue mechanical stress or shock; and
- do not immerse it in liquid.

11 PERIMETER EMAIL FILTERING

Senate office expectations are that electronic messages including file attachments will be kept private except as authorized by the owner, sender, or recipient of the information.

Senate email users expect privacy protection against both interception of electronic communications while in transmission and against unauthorized intrusion into email stored on their systems.

The SAA respects Senate email users' privacy and does not monitor the contents of their email communications unless specifically requested in writing by the Senator or Office Head and authorized by the SAA. In that instance, monitoring is performed on the requesting Office's data

as authorized and only for a limited length of time. All monitoring information is turned over to the requesting office. No monitoring data is retained on file by the SAA.

To protect the integrity of transmitted information and the integrity of Senate office systems, software programs may be used at the network perimeter to monitor email traffic for the presence of computer viruses, network worms, and other malicious code. These programs only examine email data for the presence of specific hostile code signatures.

If a perimeter scanning program detects a code signature in an email message or attachment, the hostile code will be removed and the sanitized message forwarded to the recipient. If the code cannot be removed, the recipient will be notified that the message contained a virus or other malicious code. The message will be quarantined (or deleted). No information on the content of the scanned messages or attachments is retained by the SAA.

In the case of global threats where a hostile code signature has not yet been identified, mail from a specific network address, with a specific header text or with a specific file attachment may be intercepted and quarantined (or deleted). This action will be taken for critical or unusual events that could compromise the quality, utility, or functionality of SAA services and operations and which may result in information loss or compromise, service denial or disruption for Senate users.

12 ACCESS TO RESTRICTED AREAS

Sergeant at Arms (SAA) employees and non-SAA personnel with access to restricted areas of the Capitol or Senate office buildings are responsible for understanding and following adopted security practices and procedures, and notifying appropriate management of security violations and problems. SAA and contractor staff are expected to maintain the security in any access-controlled area by not allowing unauthorized entry. Any unusual events, suspicious individuals, or illegal activities are to be reported to the Capitol Police immediately.

13 SENATE ID CARD

All Senate staff are issued a photo identification card, commonly referred to as a Senate ID card. This card is renewed at the beginning of each Congress. Senate contract staff receive special identification cards (different color border) valid for the period they are on assignment to the Senate.

The Senate ID card is always to be worn and readily visible while within restricted access areas of the Capitol and office buildings. Individuals displaying a Senate ID card may use any entrance to

the Capitol and the Congressional office buildings. Contractor access to some areas is limited to normal business hours. In the case of the Postal Square building, once the cardholder is inside of the building, the Senate ID card will allow entry to Sergeant at Arms Office space.
A Senate ID card in the possession of anyone other than the individual to whom it was issued will be confiscated by the Capitol Police. A police report will be filed, the individual's supervisor notified, and the card will be voided.

The Senate ID card must be surrendered upon termination of employment or assignment to the Senate. Supervisors are responsible for ensuring that cards from terminating staff, including contract staff, are returned.

Report lost or stolen cards immediately to the Senate ID Office. To obtain a replacement card, a form must be filed with the ID Office. A new card will be issued three days after the form is received.

13.1 Postal Square Sixth Floor and Other Senate Site Access

Staff working on the sixth floor of Postal Square or at other Senate sites are issued ID cards that are programmed for the proximity readers located in such areas. The security is controlled by the U. S. Capitol Police. Access to restricted areas at such locations is determined by the zones coded into the ID card. Requests for changes to the coded access level should be directed through a Branch Manager to the Director of Enterprise Operations.

The below ID card holder's requirements should be followed.

- Use the ID card only to gain access in the regular performance of duty. Any other use constitutes a security violation and may result in disciplinary action or legal prosecution. An ID card in the possession of anyone other than the individual to whom the card is issued will be confiscated by the Capitol Police. A report will be filed, and the matter turned over to the Sergeant at Arms for disciplinary action.
- Ensure that all doors used to gain access by proximity reader are properly closed and secured after each use.
- Contact Capitol Police immediately any time the security of a restricted area is in question.
- Report lost, stolen, or defective ID cards to your supervisor or Contracting Officer Technical Representative who will then report the issue to SAA Admin Facilities at Admin_Facilities@saa.senate.gov. Lost or stolen ID cards must be reported immediately so the access codes can be deactivated. If the ID card is subsequently recovered after a new one is issued, turn it in to SAA Administrative Services.

13.2 Care of ID Cards

The Senate ID Cards contain components which are sensitive to severe stress or temperature. To assure long badge life avoid the following actions:

- Putting the card in a back pocket, unprotected, and sitting on it;
- using the card as a tool such as a window scraper or to pry things open;
- bending the card in excess; and
- exposing the card to harsh elements such as chemicals, dirt, or water.

13.3 Postal Square Visitors

All visitors, are screened at the Bureau of Labor Statistics (BLS) First Street Desks. BLS will only accept visitor registration requests from the Senate 6th floor receptionist.

Anyone who arranges for admittance of visitors to Postal Square is responsible for those visitors and will be held accountable for their actions while in the building.

Register visitors with the Front Desk at least twenty-four hours prior to the visit. The Front Desk will accept visitor authorization only from SAA employees and contractors located at Postal Square.
SAA staff who have individuals visiting Postal Square on a regular basis may request that those individuals be placed on the Frequent Visitors List. Persons on this list will be admitted during regular BLS business hours without prior registration. Contact SAA Administration for information on how to add a visitor to this list.

Unplanned visitors or those who are not preauthorized can arrange for immediate admittance by providing a contact name and phone number of staff stationed at Postal Square. If the Senate staff contact is not available, the visitors will not be admitted.

Discuss special needs, such as open seminars where the names of expected visitors may not be known, with SAA Administrative Services well in advance of the visit.

During BLS security hours (6:00 p.m. to 6:00 a.m., Monday through Friday, Saturday, Sunday and Holidays), visitors must be verified and escorted by a SAA employee to and from the BLS security desk. Outside of BLS security hours, visitors who are unable to provide proper identification and obtain a certified escort will be denied access to the building.

13.4 Postal Square Data Center

ID card Access to the PSQ Data Center is restricted to only those SAA and contractor employees whose work responsibilities require their frequent and regular presence in the area. These

individuals may temporarily admit visitors to the Data Center provided such visitors are escorted by authorized Senate staff while in the area. A Visitors Log is maintained at each entrance to the Data Center.

Staff admitting visitors into the Data Center are responsible for those visitors and will be held accountable for their actions while in the facility. It is their responsibility to escort the visitors and to ensure that they sign the Data Center Visitors Log. All persons receiving temporary access must sign the visitor's log when they first enter and sign out when they leave the area for the day.

Tours, presentations, or any other activity involving the presence of groups of people in the Data Center require prior approval from the Director of Enterprise Operations. Notify the supervisors of the sections located in this facility when the group will be visiting.

Photographing, filming, or videotaping is not allowed in this area without the permission of the Committee on Rules and Administration.

14 CONTRACTOR RESPONSIBILITIES FOR CYBERSECURITY

For contractor products (hardware and/or software) and/or services (CPS) supplied to the Senate, the contractor shall adhere to all relevant US Government standards for cybersecurity including but not limited to the latest published revisions of US Department of Commerce National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications (SP) including, but not limited to, the following SPs:

- NIST SP800-53 Rev 5 - Security and Privacy Controls for Information Systems and Organizations;
- NIST SP800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations; and
- NIST SP800-171 Rev 2 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

Contractor shall ensure that products that it supplies to the Senate incorporate and are maintained at the latest revision levels of applicable operating system and other cybersecurity and system management component software. Such software shall include non-prohibited endpoint protection software that adheres to US federal standards for such software and may include the endpoint protection software components that are supported by the Senate for its own computer systems including but not limited to Carbon Black, Symantec Endpoint Protection, JAMF, Lookout, and Tenable.

Contractor shall conduct a risk assessment (RA) on all new products and/or services prior to offering them to Senate offices. Such RA's shall be performed in accordance with NIST standards and practices for conducting and documenting risk assessments, the contractor shall include the SAA Cybersecurity Department throughout the risk assessment process, and the results of such RA's shall be submitted to the Senate Cybersecurity Department for review and approval. Included within the scope of this requirement, are third party software components (e.g. opensource) and product plugins (e.g. for web browsers or for extending software capabilities).

Contractor shall ensure that products that it supplies to the Senate are maintained to the latest software security update level in accordance with the timeframes established in Section **14.3.12 – Software Updates and Patches** of this SOP.

Contractor shall perform regular security control reviews of its corporate system(s) and shall ensure that all hardware and software security updates (including, but not limited to, anti-virus definition updates, operating system and application security patches, firmware updates, and

related actions) and any other remediation processes deemed necessary by the SAA are tested and applied prior to connecting said systems to the Senate IT infrastructure.

Systems (including, but not limited to, hardware, software, firmware, cloud, or related systems) that are not required to support performance of the Contract of which this SOP forms a part shall not be installed by the Contractor in the Senate IT environment unless such systems are first identified and approved in writing by the SAA.

The SAA shall reserve the right to perform or have a third party perform, as necessary, vulnerability assessments and any other analysis of Contractor system(s) used within the Senate IT environment and take any necessary action to ensure that these systems do not threaten the confidentiality, integrity, or availability of Senate information systems. The Contractor shall remediate any issues raised by the SAA in a manner approved by the SAA Cybersecurity Department prior to returning systems to normal operations within the Senate environment.

The Contractor's cybersecurity measures, policies, and procedures must ensure Senate data integrity, confidentiality, and availability. The controls specified in this section of the SOP are the Senate's general cybersecurity requirements. The Contractor shall review, acknowledge and inform the Senate in its proposal how it will meet the security controls as listed herein. The Contractor is required to amend its security policies and procedures as necessitated by changes in the Senate's cyber security rules and policies. The requirements apply to all CPS provided to the Senate by the Contractor.

The remainder of this section consists of three sub-sections: Contractor Access to Senate Systems and Services, Contractor Security Plan (CSP), and Contractor Cybersecurity Measures, Policies, and Procedures. These requirements follow the guidelines that can be found in the NIST Special Publication 800-53 Revision 5 and other related NIST Special Publications on Cybersecurity. Contractors should reference those documents when constructing their response to these requirements. The Senate will designate a Contracting Officer Technical Representative (COR) for each contract for which this section of the SOP is applicable.

Contractor shall, always, be compliant with the requirements specified herein.

14.1 Contractor Access to Senate Systems and Services

Contractors must be briefed on SAA security policies and procedures and all Contractor staff who access Senate systems must successfully complete the standard SAA-provided annual Cybersecurity Awareness training. In performance of a contract, it is sometimes necessary for contractor personnel to have privileged access to Senate information technology resources.

Direct access to hardware, software or data files may be needed for problem diagnosis, maintenance, general support or for the implementation of new applications.

Contractor staff must be well trained and trustworthy. They are accountable for any unauthorized, negligent, or willful actions in violation of access privileges. These include but are not limited to:

- exploration or exploitation of a Senate system;
- introduction of malicious software;
- unauthorized modification or disclosure of a system or data;
- unauthorized copying of software or data;
- disclosure of passwords or other information relating to accessing a Senate system; and
- failure to properly log off a Senate system or take other precautions against unauthorized access.

The level of security achieved depends upon the honesty and ability of individuals who have privileged access. Therefore, all contractor staff assigned to work on Senate contracts requiring privileged access will:

- undergo a background investigation;
- provide a resume for evaluation of qualifications and competence to perform assigned duties; and
- sign an information security acknowledgment statement acknowledging the obligation to protect Senate information from improper disclosure or misuse.

Access badges will be issued to contractor staff who require access to restricted areas. The access badges and Senate identification cards must be surrendered when contractor staff are no longer assigned to the Senate.

14.1.1 SAA Systems and Services

Contractor access to Senate information technology resources is restricted to what is required to carry out contractual responsibilities. Contractors may access a Senate application only under the conditions specified by the office running that application. They may not access user data files unless specifically authorized by the information owner. All access privileges to SAA systems and services are terminated upon notification that personnel are no longer assigned to a Senate contract.

Contractors using Senate networks may access only office systems or central services for which they have been authorized.

14.1.2 Senate Office Systems

Senate offices are responsible for controlling access to their own computer systems both locally and remotely. Support contractors require access to these systems, but the office controls the extent and degree of access. Each office must weigh for itself the risks of providing broad contractor access against the necessity of sustaining efficient, reliable system operations.

In all cases, contractors access an office system only when they have been granted specific permission by the office. The permission takes the form of the office providing the contractor with a logon ID and password combination to allow access. Once logged onto a Senate office system, contractors may have privileged administrator capabilities so they can resolve critical problems. They can access anything the System Administrator can access. The System Administrator is responsible for monitoring all work performed by a contractor and ensuring that access privileges are not misused.

Remote access increases risk but, it may be necessary at times when problems cannot be resolved over the phone and someone cannot quickly or easily be dispatched to an office. System unavailability for the length of time needed for a technician to travel to the office, log on the system, diagnose, and correct the problem is not acceptable for many offices. In these instances, remote access can represent an acceptable risk for timely resolution of an acute problem.

Offices are advised to establish a special account for contractors that is activated only when remote support requiring high-level privileges is needed. The password should be changed after each support effort so that access is allowed only for a limited period. Offices are cautioned to closely monitor system activity at times when this account is used.

14.2 Contractor Cybersecurity Plan

The Contractor will provide a comprehensive contractor cybersecurity plan (CSP) in their proposal which address the security controls listed below. The Contractor shall revise their plan as requested by the Senate. The COR retains the right to request that the CSP be updated when required to match changes in the Senate's security controls posture. The controls are referenced to items within NIST Special Publication 800-53 Revision 5.

14.2.1 Least Privilege Model

The CSP shall enumerate a least privileged model to restrict access to the CPS system and Senate data.

14.2.2 Configuration Management

The CSP shall explain how it will perform configuration management of the CPS.

14.2.3 Maintenance Policies and Procedures

The CSP shall detail Contractor's maintenance policies and procedures.

14.2.4 Technician Training and Authorization

The CSP shall provide details on training and authorization of technician's in the maintenance and upgrading of CPS systems with respect to protecting Senate data.

14.2.5 Third Party Security Requirements

The CSP must detail Contractor's plan for security requirements for third party personnel.

14.2.6 Developer Security Test Plan

The CSP shall address the creation and execution of a developer security test plan.

14.2.7 Supply Chain Security

The CSP shall address its plans to protect Senate data with respect to its supply chain (third-party providers and sub-contractors).

14.2.8 Incident Response Plan

The contractor shall include in the CSP their plans for detecting, responding, and recovering from security incidents involving their corporate IT assets and network. Contractors should refer to NIST SP-800 61 for further information.

14.3 Contractor Cybersecurity Measures, Policies, and Procedures

The Contractor's Cybersecurity measures, policies, and procedures must ensure Senate data integrity, confidentiality, and availability. The following controls are the Senate's general cybersecurity requirements. The Contractor shall review, acknowledge, and inform the Senate in its CSP how it will meet the security controls as listed herein. The Contractor is required to amend its cybersecurity policies and procedures as necessitated by changes in the Senate's cybersecurity rules and policies.

The CSP shall include policies, technologies, trained staff, processes, and management/technical/operational controls that are fully implemented, tested regularly, and enforced.

Specifically, these controls shall effectively protect the integrity, confidentiality, and availability of 1) all Senate logon credentials and associated software issued to the Contractor (e.g. local admin accounts, user accounts, VPN software and tokens), 2) Senate data, applications and systems in the Senate IT environment, 3) the Contractor's CPS application software development environment and code base used for Senate customer Systems, and 4) corporate

IT assets (including Contractor IT systems used for remote access to the Senate network). The Contractor shall regularly assess, test and update their security controls to effectively protect against external and internal threats.

14.3.1 Corporate Responsibility

14.3.1.1 Company Contact for Cybersecurity

Contractor must provide the name and contact information of the individual responsible for overall cybersecurity for their company.

14.3.1.2 Software Inventory

Contractor shall provide and maintain a current list of all software components used in their CPS applications with version identifiers and dates.

14.3.1.3 Endpoint Protection Software

Except as otherwise specified in the contract of which this SOP forms a part, the contractor shall ensure that Endpoint Protection software is installed and maintained on all CPS devices in accordance with Senate Cybersecurity Policy and this SOP.

14.3.2 Data Protection

14.3.2.1 Critical CPS Data Backup/Restoration

Contractor must assure that all provision for the backup/restoration of critical CPS data is incorporated into the back-up/restore methodology.

14.3.2.2 Recovery Time Requirements

Contractor must define "time to recovery" objectives for CPS and assure completeness of recovery.

14.3.3 Media Protection

14.3.3.1 Certification of Media

Contractor must certify that all systems/media used for installation/maintenance of the CPS are free of malicious code.

14.3.4 Personnel Security Controls

The Contractor is required to ensure that all personnel with access to Senate information are authorized to do so and will have controls in place to prevent access to Senate information by unauthorized personnel.

If requested by the COR, the Contractor will further submit information pertinent to personnel security to the COR for review of its sufficiency and adequacy to meet the objectives of this Contract and will promptly make those changes requested by the COR after the review.

14.3.5 Cybersecurity Incident Response Plan and Procedures

14.3.5.1 Incident Response Plan and Procedures Requirements

The Contractor is required to establish and implement a corporate cybersecurity incident response plan and procedures (IRPP). The Contractor's IRPP shall include documented procedures for promptly and effectively preparing for, detecting, reporting, investigating, containing, remediating and recovering from security incidents involving their corporate IT assets. The IRPP shall also include the procedure for notifying the Senate of a corporate cybersecurity incident.

14.3.5.2 IRPP Review and Approval

The Contractor shall submit their IRPP to the COR for review of its sufficiency or adequacy to meet the objectives of the Contract and will promptly make those changes requested by the COR after the review.

14.3.5.3 Cybersecurity Incident Reporting

The Contractor shall immediately notify the COR and the Senate's Cyber Security Operations Center (CSOC)* of:

1. any suspected security incident affecting their IT environment which could result in a compromise of the confidentiality, integrity or availability of CPS provided to the Senate;
2. any attempt to access the Senate network using Contractor resources or Senate-issued credentials that is not authorized for legitimate business purposes as set forth by the contract;
3. any suspected cybersecurity incident which could result in unauthorized access to Senate data; or

4. any suspected cybersecurity incident which may compromise Contractor IT systems used to connect to the Senate network.

The Contractor shall provide prompt updates to the Senate as additional incident details emerge and/or as requested by the SAA.

* Cyber Security Operations Center (CSOC) phone number: 202-228-2927, Option 1. Email: csoc@saa.senate.gov.

14.3.6 Cybersecurity Training

The Contractor shall deliver cybersecurity training for all Contractor staff regarding safeguarding customer information and the procedures which must be followed to ensure the protection of that information. The training must ensure that employees understand their responsibilities for safeguarding Senate information and incorporate effective security practices as a part of their day-to-day activities. The implementation features that would be required to be incorporated are as follows:

1. Cybersecurity and physical awareness training for all personnel, including management.
2. Periodic cybersecurity reminders.
3. User education concerning protection against malicious code and spear-phishing;
4. User education in importance of monitoring login success/failure, and how to report discrepancies.
5. User education in password management.
6. Incident response notification process.

14.3.7 Chain of Trust Partner Agreement

If data are processed through a third party, including but not limited to, suppliers, subcontractors, or other companies working with the Contractor, each such third party will be required to enter into a “chain of trust partner” (COTP) agreement. Under this COTP agreement, the Contractor and any associated parties will agree to exchange data and to protect the transmitted data in accordance with the Cybersecurity requirements set forth in the Contract and the Contractor’s approved CSP. These agreements will ensure that information remains secure whenever it moves from one organization to another. The Contractor will submit the COTP agreement to the Contracting Officer for review of its sufficiency or adequacy to meet the objectives of the Contract and will make those reasonable changes requested by the Contracting Officer after the review.

14.3.8 Remote Access

14.3.8.1 Remote Access Authorization

Offices consenting to the Contractor's remote access to the office's network and associated networked devices for purposes of troubleshooting and support must provide a signed form to the COR authorizing such access (See Section 15 below, *Senate System Remote Access Authorization Form*) before the access will be granted. The COR will provide the Contractor with a copy of this authorization. The Contractor's remote access shall be subject to any conditions noted by the Senate office on the form. Offices can revoke such authorization at any time and the Contractor's remote access will be terminated.

Contractor shall ensure that any keys, tokens, proximity cards, credentials, or IDs issued by the Senate for a specified employee's use are not shared with other persons or reassigned to other employees upon the employee's termination.

14.3.8.2 Remote Access Procedures

Senate offices must authorize the Contractor's remote access to the CPS by signing the Senate System *Remote Access Authorization Form*. Remote access to other office computer systems and devices (both in Washington, D.C., and the state) must be orally authorized by the office staff on an "as needed" basis, per the procedures below.

1. The ticket is assigned to the appropriate technician via the Senate Service Manager (SSM);
2. Technician contacts User and/or SA to further troubleshoot.
    a. If user is unavailable, the technician leaves a voicemail, with ticket number and a request to call back.
    b. The technician tracks all communication with the user and/or SA via the SSM.
3. The technician requests permission from User and/or SA to connect to system remotely.
4. If permission is granted, the technician connects to the system,
5. The technician performs troubleshooting, applies resolution and tests functionality.
6. The technician documents all work in the SSM.
7. The technician terminates the Connectivity session.
8. The technician assists the user with stopping the connectivity host.
9. The technician does not document any usernames, passwords, or IP Addresses.

14.3.8.3 Remote Access Support from Non-Senate Locations

To ensure the security of the Senate network, the SAA reserves the right to suspend the Contractor's remote access to the Senate network if a cybersecurity threat is identified. If the Contractor's remote access is suspended, the Contractor shall continue to provide the services specified in the contract. The SAA will determine the circumstances under which the Contractor's

remote access capability may be restored.

14.3.9 Contractor Accounts

14.3.9.1 Contractor Logon Account

The Contractor shall establish a logon account for use by the Contractor's technicians while performing support activities such as system maintenance, upgrades, or Help Desk support on the CPS server or servers. This account must have local administrator rights to the CPS server or servers. Under no circumstances may the Contractor request, establish or use domain administrator accounts or any other accounts with administrative privileges.

14.3.9.2 Contractor Domain Account

If the Contractor requires a domain user level account for support activities on systems other than the CPS server or servers, the Contractor must receive approval from the COR before such accounts are established. To request approval, the contractor must submit a formal written request explaining why a domain user account is needed and how it will be used. If approved, the Contractor shall request the domain user account from the office system administrator. Under no circumstances may the Contractor request, establish or use domain administrator accounts or any other accounts with administrative privileges.

14.3.9.3 Contractor Password Security

The Contractor shall be responsible for ensuring the security of passwords for their local administrator accounts and domain user accounts (if applicable). The Contractor must implement a documented process for changing the password for these accounts on a regular basis, but the password must be changed no less frequently than one (1) time per quarter and must meet the following criteria:

- the password must contain at least 12 characters,
- the password cannot contain the username or the word “password”,
- the password cannot re-use any of the last 12 passwords, and
- the password must contain at least 3 of the following 4 criteria:
    - upper case letters (A-Z),
    - lower case letters (a-z),
    - numeric (0-9), and
    - non-alphanumeric or special characters (e.g. *&%!+).

14.3.9.4 Contractor Password Maintenance Report

Unless otherwise agreed to in the contract incorporating this SOP, The contractor shall deliver a report to the Contracting Officer and the COR, not later than ten calendar days after the first of the month beginning a new quarter, which provides the Contractor's attestation that the passwords have been changed for each of the accounts used to support and maintain offices' CPS systems as described above.

14.3.9.5 Contractor Accounts Scope of Use

The Contractor's local administrator account and domain user accounts (if applicable) shall only be used by the Contractor's technicians in conjunction with support activities related to or involving the CPS.

14.3.9.6 Contractor Account Standard Naming Convention

The Contractor shall work with the COR following contract award to establish a standard naming convention(s) for the Contractor's accounts.

14.3.9.7 Elevated Privilege Contractor Accounts Password Management

Except as agreed to by the Senate COR, all Contractor accounts with elevated privileges must be implemented using the Senate Privileged Account Management (PAM) Service with automatic password rotation.

14.3.10 Continuity of Operations Plan

Contractor must meet Senate requirements for the Contractor's continuity of operations plan (COOP)

14.3.10.1 General Requirement

The Senate has as its policy a requirement for the Contractor to have in place a comprehensive and effective program to ensure the continuity of both their Senate customers' and their own essential functions under all circumstances.

14.3.10.2 Business Continuity Plan

The Contractor, as a provider of activities or capabilities which support the Senate's essential functions, must provide the Senate with a business continuity plan detailing procedures and advance arrangements that will enable the Contractor to respond to and recover from a disruptive event that affects:

1. The Contractor's staff
2. The Contractor's place of business
3. The Senate's staff
4. The Senate's place of business, or
5. Any combination of the above.

14.3.10.3 Minimum Requirements

At minimum the continuity plans must describe:

1. How the Contractor intends to notify the Senate of a disaster that affects the Contractor's staff or place of business and its impact on the Contractor's business operations;

2. How the Contractor expects to be notified of a disaster that affects the Senate's staff or place of business;

3. What provisions the Contractor has made for the Senate to contact Contractor personnel in a disaster;

4. How the Contractor intends to re-establish the delivery of materials and services to the Senate;

5. How the Contractor intends to provide Senate offices with continued access;

6. A COOP solution for CPS systems installed on dedicated CPS servers (physical or virtual servers) installed on offices' networks that fully accomplishes application fail-over for all application components, i.e., database, files, email, faxes, etc. In the event of a failure or outage, all application features and functionality must continue to be available to all users in all sites. Note that there is no requirement that application failover be automatic; however, the failover must be easily accomplished;

7. Alternate operating facilities from which the Contractor's services provided to the Senate can continue;

8. Logistics for the receipt and delivery of orders to the Senate if Contractor is operating from an alternate facility; and

9. The process for testing of the COOP plan at least annually. This COOP plan and the process for testing will be agreed between the Contractor and the Senate within 60 calendar days of the signature date of the contract of which this SOP is a part.

14.3.10.4 Senate Review and Approval of COOP Plans

The Contractor shall submit its COOP plans to the Senate. The Senate will review and approve these COOP plans based on the criteria listed above. If the Contractor's COOP plan is not accepted by the Senate, the Contractor must revise the plan until it meets Senate requirements.

14.3.11 Personnel Termination Procedures

The Contractor shall implement termination procedures, which are formal, documented instructions that include appropriate security measures for ending either an employee's employment or an internal/external user's access. These procedures must prevent the possibility of unauthorized access to Senate data, networks, or systems by those who are no longer authorized.

Termination procedures shall include, but are not limited to, the following mandatory controls at a minimum:

1. Promptly notifying the COR of the employee's pending employment termination (including their last day of employment).

2. Immediate removal from all access lists.

3. Disabling of all user account(s).

4. Immediate recovery or disabling of all keys, tokens, Senate Furnished Equipment (SFE) proximity cards, or IDs that allow access to either the Contractor's or the Senate's network or physical office locations.

5. Promptly returning to the COR any keys, tokens, Senate SFE, proximity cards, or IDs issued by the Senate for the terminated employee's use.

14.3.12 Software Updates and Patches

Contractor must perform system maintenance including applying software patches and updates (as approved by the SAA).

14.3.12.1 Software Maintained at the Most Current Patch State

The Contractor is responsible for ensuring that the CPS, as well as any 3rd party software used by the CPS, are maintained at the most current patch state. The Contractor is also responsible for testing and ensuring CPS compatibility with all patches/updates to any software used in the operation of the Contractor's CPS (on workstations and servers).

With respect to software updates and patches that remediate known vulnerabilities, the timeframes established in Table 14.3.12.1-1 below must be adhered to by the contractor for deployment of such remediation. These timeframes are measured starting with the date of release of the software update or patch from the affected software supplier.

Common Vulnerability Scoring System		Remediation Timeframe (Calendar Days)
Qualitative Severity Level	Numerical Score Range	
Critical	9.0 - 10.0	1
High	7.0 - 8.9	7
Medium	4.0 – 6.9	14
Low	.1 – 3.9	28

Table 14.3.12.1-1 – Software Vulnerability Remediation Timeframes
Ref: https://www.first.org/cvss/v3.1/specification-document

Failure to achieve the timeframes specified in Table 14.3.2.1-1 for remediation of a security update or patch will be deemed a material breach of the contract of which this SOP is a part unless the cause of such failure is due to delays caused by the Senate.

14.3.12.2 Inventory and History of Contractor Applied Patches

The Contractor is also responsible for maintaining a history of Contractor applied patches, and must be able to provide a software/system inventory.

14.3.12.3 Deployment of Security Patches and Software Updates.

To ensure that security patches and other software updates are applied to Senate systems as promptly as possible, software patches and updates are deployed by the SAA as follows:

a) Windows Server Update Services (WSUS) is a Microsoft (MS) critical patch deployment solution providing the automated, scheduled "push" (currently download only to servers) of critical Microsoft updates to the recipient systems (servers and workstations) that are running Windows operating systems. The following MS applications are currently included in the Senate's SUS updates: Windows, Windows Server, Office Productivity Suite, Edge, and SharePoint.

b) System Management Service (SMS) is a critical patch deployment system providing the automated, scheduled "push" of security patches/updates for a variety of third-party applications to recipient systems (workstations only), currently including the following: Adobe Acrobat & Reader, Oracle Java, Mozilla Firefox, VLC Media Player, and Apple QuickTime.

c) Symantec Endpoint Protection (SEP) patches are released through the Senate's Symantec update process, and are pushed to the recipient systems (servers and workstations). The COR will notify the Contractor in advance about the pending release of Symantec patches and/or updates.

d) Carbon Black (CB) patches are released through the Senate's Carbon Black update process, and are pushed to the recipient systems (servers and workstations). The COR will notify the Contractor in advance about the pending release of Carbon Black patches and/or updates.

e) Security patches and updates for software not patched via the Senate's automated patch deployment systems are applied/installed manually.

14.3.12.4 Additional Contractor Requirements

a) Notify the COR of the release of any CPS security patches/updates, as well as all security patches/updates for any third-party software (including CPS database software) used in the Contractor's CPS, within 24 hours of their release;

b) Ensure that all security patches/updates for software used in the operation of the Contractor's CPS (on workstations and servers) are properly tested by the Contractor within 48 hours* of their release;

c) Report any patch/update incompatibility to the COR (or designee) within 48 hours* of their release;

d) Install/apply on all customer CPS servers all CPS security patches/updates, as well as all security patches/updates for any third-party software (including CPS database software) used in the Contractor's CPS within 72 hours* of their release, and then verify CPS functionality; and

e) Notify the COR when the installation/application of any CPS security patch/update, or third-party software (including CPS database software) security patch/update used in the Contractor's CPS, on all customer CPS servers is complete.

* There may be emergency situations that warrant an accelerated/shortened patch/update testing, reporting and installation/application schedule. The COR will promptly notify the Contractor when such emergencies are identified and will provide the accelerated schedule.

14.3.13 Cloud Service Use

This section of the SOP provides the contractor requirements for the use of Cloud Computing Services in the fulfillment of contracts for CPS as defined in this SOP.

14.3.13.1 Definitions

"Authorizing official," means the senior Senate official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

"Cloud computing" means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

“Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

“CPS” means products (hardware and/or software) and/or services supplied to the Senate by a contractor.

“Senate data” means any information, document, media, or machine-readable material regardless of physical form or characteristics, that is created or obtained by the Senate in the course of official Senate business.

“Senate-related data” means any information, document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Senate data. This does not include contractor’s business records e.g. financial records, legal records etc. or data such as operating procedures, software coding or algorithms that are not uniquely applied to the Senate data.

“Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

“Media” means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

“Spillage” security incident that results in the transfer of classified or controlled unclassified information onto an information system not accredited (i.e., authorized) for the appropriate security level.

14.3.13.2 Cloud computing security requirements

The requirements specified herein are applicable when using cloud computing to provide information technology services in the performance of the contract of which this SOP is a part.

14.3.13.2.1 Use of Cloud Computing

If the Contractor indicated in its offer that it “does not anticipate the use of cloud computing services in the performance of a resultant contract,” in response to a solicitation from the Senate

incorporating the requirements herein, and, after the award of the contract, the Contractor proposes to use cloud computing services in the performance of the contract, the Contractor shall obtain approval from the Contracting Officer prior to utilizing cloud computing services in performance of the contract.

If the CPS incorporates the use of Cloud Services (CS) then, except as otherwise agreed to in the contract of which this SOP is a part, the underlying CS infrastructure that is used by the Contractor to deliver such CPS must meet the following specifications:

14.3.13.2.1.1 **FedRAMP Impact Level Requirement**

- The CS is authorized at a FedRAMP Impact Level of Moderate or High.

14.3.13.2.2 Maintenance of required administrative, technical, and physical safeguards and controls

The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the SOP for Cybersecurity in effect at the time the solicitation is issued and as updated from time to time or as authorized by the Contracting Officer, unless notified by the Contracting Officer that this requirement has been waived by the Senate SAA Chief Information Officer.

At the request of the COR, the Contractor shall provide the Senate with a CS account with auditor (read only) level access to the Contactor's CS environment for performing an audit of the contractor's security controls as applied to the CS infrastructure that the Contractor has delivered in accordance with the contract of which this SOP forms a part.

14.3.13.2.3 Geographic Location of Senate Data

The Contractor shall maintain within the area of the United States or outlying areas, all Senate data that is not physically located on Senate premises, unless the Contractor receives written notification from the Contracting Officer to use another location outside of this area.

14.3.13.3 Limitations on access to, use, and disclosure of Senate data and Senate-related data

14.3.13.3.1 Authorized Use and Disclosure of Senate Data

The Contractor shall not access, use, or disclose Senate data unless specifically authorized by the terms of the contract or a task order or delivery order issued and incorporating this SOP.

14.3.13.3.1.1 Scope of Authorized Use of Senate Data

If authorized by the terms of the contract or a task order or delivery order issued hereunder, any access to, or use, or disclosure of Senate data shall only be for purposes specified in the contract or task order or delivery order incorporating this SOP.

14.3.13.3.1.2 Contractor Employee Obligations

The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

14.3.13.3.1.3 Survival on Contract Termination or Expiration

These access, use, and disclosure prohibitions and obligations shall survive the expiration or termination of the contract incorporating this SOP.

14.3.13.3.1.4 Scope of Authorized Use of Senate-related Data

The Contractor shall use Senate-related data only to manage the operational environment that supports the Senate data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

14.3.13.3.1.5 Cloud Computing Services Cyber Incident Reporting

The Contractor shall report in accordance with this SOP all cyber incidents that are related to the cloud computing service provided to the Senate by the contractor.

14.3.13.4 Malicious software

The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided in the SOP.

14.3.13.5 Media preservation and protection

When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in the associate cyber incident report and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow the Senate to request the media or decline interest.

14.3.13.6 Access to additional information or equipment necessary for forensic analysis

Upon request by the COR, the Contractor shall provide the Senate with access to additional information or equipment that is necessary to conduct a forensic analysis.

14.3.13.7 Cyber incident damage assessment activities

If the Senate elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all damage assessment information gathered in accordance with this SOP.

14.3.13.8 Records management and facility access

14.3.13.8.1 Records Format Requirements

The Contractor shall provide the Contracting Officer all requested Senate data and Senate-related data in the format specified in the contract incorporating this SOP.

14.3.13.8.2 Data Disposal

The Contractor shall dispose of Senate data and Senate-related data in accordance with the terms of the contract incorporating this SOP and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

14.3.13.8.3 Senate Access to Data

The Contractor shall provide the Senate, or its authorized representatives, access to all Senate data and Senate-related data, access to contractor personnel involved in performance of the contract, and physical access to any Contractor facility with Senate data, for the purpose of audits, investigations, inspections, or other similar activities, as authorized by law or regulation.

14.3.13.9 Notification of *third-party* access requests

The Contractor shall notify the Contracting Officer promptly of any requests from a third party for access to Senate data or Senate-related data, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or local agency. The Contractor shall cooperate with the Contracting Officer to take all measures to protect Senate data and Senate-related data from any unauthorized disclosure.

14.3.13.10 Spillage

Upon notification by the Senate of a spillage, or upon the Contractor's discovery of a spillage, the Contractor shall cooperate with the Contracting Officer to address the spillage in compliance with Senate procedures.

14.3.13.11 Subcontract*s*

The Contractor shall include SOP clause 14.3.13 Cloud Service Use, including this paragraph 14.3.13.11, in all subcontracts that involve or may involve cloud services, including subcontracts for commercial items.

14.3.14 Breach Notification

If the Contractor, or its subcontractors or third party partners, learn of any incident of unauthorized access to or data breach of any Senate data in performance of the contract of which this SOP forms a part, the Contractor will, within 72 hours of an incident, report such incident to the SAA Cyber Security Operations Center (CSOC) at (202) 228-2927, option 1, or csoc@saa.senate.gov. This notification requirement applies, whether the incident is identified by the Contractor itself or is brought to the Contractor's attention by a third party. The Contractor will use the US DHS/CISA Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines for guidance on definitions. "Incidents" include, but are not limited to:

a) any suspected incident affecting the Contractor's IT environment which could result in a compromise of the confidentiality, integrity, or availability of the Products and/or Services provided to the Senate by the Contractor; and

b) any suspected incident which could result in unauthorized access to Senate data.

The initial notification from the Contractor to the CSOC concerning the incident shall include:

1. Identification of

- the current level of impact on Senate functions or services (Functional Impact),
- the type of information lost, compromised, or corrupted (Information Impact),
- when the activity was first detected,
- the number of systems, records, and users impacted,
- the network location of the observed activity,
- point of contact information for additional follow-up,
- attack vector(s) that led to the incident (if available),
- indicators of compromise, including signatures or detection measures developed,
- mitigation activities undertaken in response to the incident.

2. Estimation of the scope of time and resources needed to recover from the incident (Recoverability).

After the initial notification, the Contractor shall provide daily updates to the CSOC until all incident related issues have been satisfactorily resolved and all incident related actions have been satisfactorily completed. Incident details to be reported to the CSOC in such daily updates will include at least the following data points:

- Is Senate data affected and if so, what data;
- Is the Senate network affected, and, if so, what network components;
- Are Senate accounts affected, and, if so, what accounts;

- Did affected accounts have access to the Senate network;
- Was there a loss of sensitive Senate information (e.g. PII/IP Address/Design Docs/Network design info/etc.);
- What identifiable malware is associated with the incident;
- Can the Contractor share the malware that was identified;
- Provide a post Breach report detailing what happened and including a root cause analysis; and
- Document what actions are being taken to improve cybersecurity and thereby prevent this incident from re-occurring. (Lessons learned).

The Senate, as a Legislative Branch entity, is not subject to US-DHS/CISA reporting requirements. The Senate requires the Contractor to report incidents in accordance with US-DHS/CISA reporting guidelines only to the Senate SAA CSOC, and not to any other government entity.

15 SENATE SYSTEM REMOTE ACCESS AUTHORIZATION FORM

In order for the Contractor's technicians to connect to offices' CPS server(s) from a remote location for the purposes of troubleshooting, support, and application maintenance, Senate offices must first authorize remote access for their Contractor by completing this form.

The Contractor's access to non-CPS devices (PC's, file/print server, etc.) is authorized only after the Contractor's technician obtains written agreement from office staff.

If you want to authorize your Contractor's remote access to your CPS server(s), please complete this form and email it to the appropriate recipient as specified below:

Server Category	Email Recipient
Constituent Support Services (CSS)	saacss@saa.senate.gov
Non-CSS Office Servers	Office Staff Director

Authorization for Contractor Remote Access to Servers

I authorize the _____ support technicians to access our office's Server(s) from their network.

I understand that the technician will have access to the information on these Server(s). I also understand that the Contractor has agreed to the security requirements documented in their contract with the SAA, which limits this access to those technicians assigned to the Senate contract. I do understand the security risks and wish to proceed with this authorization.

Please note in the box below any additional limitations or restrictions on remote access:

Office Name:

_____

Office Authorization:

_____ _____ _____

Signature *Title* *Date*

16 CYBERSECURITY RESPONSIBILITIES ACKNOWLEDGEMENT

I, _____, have read and understand my responsibilities as a user of Senate information technology facilities. I recognize that I am obligated to maintain the confidentiality of Senate information to which I have access and that failure to comply with these responsibilities is considered a violation of Sergeant at Arms Cybersecurity Policy.

_____

Name

_____

Date

Sign and forward to your Supervisor or COR.