Contractor Security Control Assessment (CSCA)

Self-Assessment Questionnaire for Contract Service Providers

Version 1.2

May 15, 2009

Document Change Control

Version	Release Date	Summary of Changes	Name
Version 0.1	March 13, 2009	First working draft submitted to CPO.	CPO
Version 0.2	March 13, 2009	Format and minor content changes	CPO
Version 0.3	March 16, 2009	Second working draft with incorporated CPO changes	CPO
Version 0.4	March 16, 2009	Third working draft with incorporated CPO changes	CPO
Version 0.5	March 18, 2009	Final working draft with incorporated CPO suggestions	CPO
Version 0.6	April 15, 2009	Incorpoation of CPO and VA staff combined suggestions	CPO
Version 1.0	May 5, 2009	Final draft document	CPO
Version 1.1	May 5, 2009	Updates made to NIST references in Appendix A	CPO
Version 1.2	May 15, 2009	Final Review for Release	FSS, OCS

Table of Contents

Executive Summary

The Department of Veterans Affairs (VA) must comply with the Federal Information Security Management Act (FISMA) and with Office of Management and Budget (OMB) direction to ensure oversight of contractors who access, maintain, store, or transmit Veterans' sensitive information. VA established the Contractor Security Control Assessment (CSCA) to assist in defining and evaluating information security control protection mechanisms and practices used to protect Veterans' sensitive information. All contractors and contract service providers must comply with the same information security requirements as VA is recommended to do the CSCA on an annual basis.

Purpose

The purpose of this document is to provide security guidance for contractors and contract service providers in remote locations or alternative work-sites who access, maintain, store, or transmit Veterans' sensitive information. This CSCA is a checklist built around the framework of the National Institute of Standards and Technology (NIST).

Per NIST Special Publication (SP) 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*:

> "The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security to its electronic data information devices."

Scope

The protection of Veterans' sensitive information is a critical and intricate part of the overall security awareness and health of the VA organization. This CSCA will assist VA in:

- Extending VA security mandates and education to affiliated contractor agencies;
- Maintaining a record of contractor agency compliance with VA-necessitated security regulations and polices that can be included in the contract file; and
- Strengthening and improving the process of securing Veterans' sensitive information on approved information devices. (An "information device" is any device used access, maintain, store, or transmit Veterans' sensitive information, such as a workstation, home computer, laptop, Blackberry, etc.)

Attestation of Compliance

Please complete this Attestation of Compliance as a declaration of your compliance with the CSCA to protect Veterans' sensitive information.

Part 1. Person Completing This Document	
Contact Name:	
Title:	
Telephone:	
Business Address:	
Email:	

Part 2. Contractor Organization Information	
Contact Name:	
Title:	
Telephone:	
Business Address:	
Email:	

Part 2a. Relationships
Does your company have a relationship with one or more third-party service providers (e.g., gateways, web-hosting companies)? ☐ Yes ☐ No

Part 2b. Transaction Processing
How is information exchanged with VA?:

Part 3. CSCA Validation
☐ **Compliant**: All sections are complete and all questions are answered affirmatively, resulting in an overall **COMPLIANT** rating.
☐ **Non-Compliant**: Not all sections are complete and/or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating. **Target Date for Compliance**:

Part 3a. Confirmation of Compliant Status	
☐	CSCA was completed according to the instructions therein.
☐	All information within the above-referenced CSCA and in this Attestation fairly represent the results of my assessment.
☐	I have read the appropriate VA directives relative to information securityand understand that I must maintain full data security standards at all times.

Part 3b. Contracting Officer's Technical Representative (COTR) Acknowledgement	
Signature of Person Completing This Document	***Date***
Printed Name of Executive Officer	***Company***
Signature of Information Security Officer	***Date***

Action Plan for Non-compliance

Please select the appropriate "Compliant" status for each requirement. If you answer "No" to any of the requirements, please complete the table below with the necessary steps to become compliant and the date on which you will be compliant.

VA CSCA	Description of Requirement	Compliance Status (Select One)		Remediation Date and Actions (If Compliance Status is "No")
		YES	NO	
1	Install and maintain a firewall configuration.	☐	☐	
2	Host, operate, maintain, or use information devices.	☐	☐	
3	Use and regularly update antivirus software.	☐	☐	
4	Implement access controls.	☐	☐	
5	Conduct risk assessments.	☐	☐	
6	Institute information security protection.	☐	☐	
7	Privacy regulation for storage of Veterans' sensitive Information.	☐	☐	

Self-Assessment Questionnaire

Requirement 1: Install and maintain a firewall configuration

VA requires the use of firewalls as a protection mechanism to ensure the confidentiality, integrity and availability of VA information.

Question	Response: (Select One)		Comment
	YES	NO	
1. Is a firewall used and installed on devices that will store, process, and maintain Veterans' sensitive information?	☐	☐	
2. If the firewall used is a hardware device, were the vendor supplied passwords removed? (hardware includes all wireless devices and routers) *Wireless environment defaults include, but are not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and simple network management protocol (SNMP) community strings*			
3. If the firewall used is a software product:	☐	☐	
a) Is it set to download automatic updates?	☐	☐	
b) Is the firewall software product installed on your PC (i.e, McAfee, Norton)?	☐	☐	
c) Is there a personal firewall software installed on any mobile and/or employee-owned computers that have direct connectivity to the Internet (e.g., laptops used by employees) and are used to access the VA's network?	☐	☐	
4. Does the firewall monitor, restrict, and respond to inbound and outbound communications by sending notification alerts when a connection is attempted?	☐	☐	
5. Does the firewall provide email-scanning that monitors incoming and outgoing messages for viruses and security threats?	☐	☐	
6. Does the firewall prohibit direct public access between external networks and any information device component that stores Veterans' sensitive information (e.g., databases, logs, trace files)?	☐	☐	
7. Is there Wi-Fi protected access (WPA and WPA2) technology enabled for encryption and authentication when WPA-capable?	☐	☐	
8. Is there justification and documentation for any risky protocols allowed (e.g., file transfer protocol [FTP]), including the reason for the use of the protocol and security features implemented?	☐	☐	
9. Are you using Federal Information Processing Standard (FIPS) 140-2 validated encryption for storing and transferring VA sensitive information?	☐	☐	

Requirement 2: VA Information Hosting, Operation, Maintenance or Use

Question	Response: (Select One) YES	Response: (Select One) NO	Comment
1. Are you designing or developing a system or information device for or on behalf of VA?	☐	☐	
2. Are you hosting, operating, maintaining, or using an information device on behalf of the VA that contains Veterans' sensitive information? (If so, then Certification & Accreditation (C&A) is required for the information device; and all security controls outlined in the VA Handbook 6500, Appendix D are required.)	☐	☐	

Requirement 3: Use and regularly update antivirus software

Information devices with access to Veterans' sensitive information are required to implement malicious code protection that includes a capability for automatic updates and real-time scans.

Question	Response: (Select One) YES	Response: (Select One) NO	Comment
1. Is antivirus software installed on all information devices with access to Veterans' sensitive information?	☐	☐	
2. Is the antivirus programs capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware?	☐	☐	
3. Is the antivirus mechanism current, actively running, and capable of generating audit logs?	☐	☐	
4. Does the antivirus mechanism provide malicious code protection mechanisms for applications that may transfer malicious code (e.g., file transfer software, instant messaging software)?	☐	☐	
5. Are updates to malicious code protection mechanisms made whenever new releases are available?	☐	☐	
6. Are information devices with access to Veterans' sensitive information email clients and servers configured to block attachments with file extensions associated with malicious code (e.g., .pif, .vbs), and suspicious file extension combinations (e.g., .txt.vbs, .htm.exe)?	☐	☐	
7. Do you scan your systems regularly for vulnerabilities?	☐	☐	
Please identify the scanning technology you use here: 8. Are malicious code protection mechanisms: a) Appropriately updated to include the latest malicious code definitions? b) Configured to perform periodic scans of the information device, as well as real-time scans of each file, as the file is downloaded, opened, or executed?	☐ ☐ ☐	☐ ☐ ☐	

Requirement 4: Implement Access Controls

VA requires the management of information device accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The frequency for reviews of information device accounts should be documented: the review of information device accounts every 90 days for moderate- and high-impact systems; the review of information device accounts every six months for low-impact systems.

At a minimum, VA requires addressing the deactivation of all computer information device accounts in a timely manner, indicative of the information device impact level, when a change in user status occurs, regardless of platform (including personal computer, network, mainframe, firewall, router, telephone, and other miscellaneous utility information devices), such as when the account user:

- Departs the agency voluntarily or involuntarily;
- Transfers to another area within the agency;
- Is suspended;
- Goes on long-term detail; or
- Otherwise no longer has a legitimate business need for information device access.

Question	Response: (Select One)		Comment
	YES	NO	
1. Are all users identified with a unique ID before allowing them to access information device components or Veterans' sensitive information?	☐	☐	
2. In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? a) Password b) Token devices (e.g., SecureID, certifications, or public key) c) Biometrics	☐	☐	
3. Are group, shared, or generic accounts and passwords forbidden?	☐	☐	
4. Are first-time passwords set to a unique value for each user?	☐	☐	
5. Must each user change their password immediately after the first use?	☐	☐	
6. Are password procedures and policies communicated to all users who have access to Veterans' sensitive information?	☐	☐	
7. Are users required to change their passwords every 90 days?	☐	☐	
8. Are user passwords required to contain both numeric and alphabetic characters?	☐	☐	
9. Are users required to submit a new password that is different from any of the last four passwords he or she has used?	☐	☐	
10. Are repeated access attempts limited by locking out the user ID after no more than six attempts?	☐	☐	
11. If a session has been idle for more than 15 minutes, must a user re-enter the password to re-activate the terminal or session?	☐	☐	

Question	Response: (Select One)		Comment
	YES	NO	
12. Is all access to any database containing Veterans' sensitive information authenticated?	☐	☐	

Requirement 5: Conduct Risk Assessments

Risk assessments are conducted to determine the likelihood of risk to information, and whether protection mechanisms are in place to reduce risk.

Risk assessments must be conducted at VA in order to evaluate the readiness of the information device, organization, or asset that will be using Veterans' sensitive information. The risk assessments for information devices or assets with access to Veterans' sensitive information are to be updated/conducted at least every three years or whenever there is a significant change to the information device, asset or work environment that may impact the security protection of the information.

Question	Response: (Select One)		Comment
	YES	NO	
1. Has a System of Records been created per the Privacy Act of 1974?	☐	☐	
2. Has the information device used under this contract been categorized (High, Medium, Low) in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*?	☐	☐	
3. Has a risk assessment been conducted to estimate potential risks and vulnerabilities to the confidentiality, integrity, and availability of Veterans' sensitive information stored, processed, or transmitted?	☐	☐	
4. If a risk assessment has been conducted for the information device or asset, does the assessment adequately address:			
a) The magnitude of harm that could result from the unauthorized access, use, disclosure, modification, or destruction of the information and the information devices that support its operations and assets (including information and information devices managed/operated by external parties); and	☐	☐	
b) When the risk assessment was conducted (i.e., a risk assessment was performed for the information device in [month/year]?	☐	☐	
5. Does the risk assessment reflect and detail the folllowing conditions that may impact the security or accreditation status of the information device with access to VA sensitive information:	☐	☐	
a) Where the information is stored on the device;	☐	☐	
b) The work location of the information device;	☐	☐	

Question	Response: (Select One)		Comment
	YES	NO	
c) Potential access to the information device from unauthorized personnel;.and	☐	☐	
d) The latest significant changes to the information device?	☐	☐	
6. What is the risk rating of the information device, based on the risk level matrix (High, Medium, Low risk level)?			
7. Are there recommended controls/alternative options to reduce risk?	☐	☐	
8. Are risk determinations annually reviewed/updated?	☐	☐	
9. What is the impact analysis and evaluation of the information device with access to Veterans' sensitive information (High, Med, Low impact)?			
10. Were potential impacts considered in accordance with the US Patriot Act of 2001 and related Homeland Security Presidential Directives (HSPDs),?	☐	☐	
11. Have mitigation strategies been discussed with VA officials with significant information and information device responsibilities?	☐	☐	
12. If a risk assessment does not exist for this information device, will a risk assessment be conducted in accordance with NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, as part of the C&A process?	☐	☐	
13. Does a contigency plan exist for your system(s)?	☐	☐	

Requirement 6: Institute Information Security Protection

Information security is the protection of information from a wide range of threats and vulnerabilities to ensure business continuity. The framework of information security includes a minimum set of security actions needed to effectively incorporate security in the system development process.

The protection of information devices with access to Veterans' sensitive information and communications is required at the session—as opposed to packet—level by implementing session level protection where needed.

System and Communications Protection

Question	Response: (Select One)		Comment
	YES	NO	
1. Are documents or records maintained that define, either explicitly or by reference, the time period of inactivity before the information device terminates a network connection?	☐	☐	
2. Does the information device terminate a network connection at the end of a session or after the organization-defined time period of inactivity?	☐	☐	

System and Information Integrity

Question	Response: (Select One)		Comment
	YES	NO	
1. Do you use web services that utilize VA information?	☐	☐	
2. Is the output from the information device handled in accordance with applicable laws, Executive Orders (E.O.), directives, policies, regulations, standards, and operational requirements?	☐	☐	
3. Is the output from the information device retained in accordance with applicable laws, E.O.s, directives, policies, regulations, standards, and operational requirements?	☐	☐	
4. Does the organization restrict the capability to input information to the information device to authorized personnel?	☐	☐	
5. Does the information device implement spam protection by verifying that the organization: a) Employs spam protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network? b) Employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by email, email attachments, Internet access, or other common means?	☐ ☐	☐ ☐	

Physical Security

Question	Response: (Select One)		Comment
	YES	NO	
1. Is the Veterans' senstive information physically controlled and securely store in controlled areas?	☐	☐	
2. Is the information device located within an area that minimizes potential damage from physical and environmental hazards?	☐	☐	
3. Is the information device positioned within an area that minimizes the opportunity for unauthorized access?	☐	☐	
4. Are procedures in place to help all personnel easily distinguish between employees and visitors, especially in areas where Veterans' sensitive information is accessible?	☐	☐	
5. Are appropriate facility entry controls in place to limit and monitor physical access to information devices that store, process, or transmit Veterans' sensitive information?	☐	☐	
6. Is physical access controlled to prevent unauthorized individuals from observing the display output of information system devices that display information?	☐	☐	

Requirement 7: Privacy Regulation for Storage of Veterans' Sensitive Information

VA requires that the handling and retention of output of Veterans' sensitive information be in accordance with VA policy and operational requirements. Other requirements include: (a) physical control and secure storage of the information media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media; and (b) utilizing alternative sites for the storage of backup information. Information devices with access to Veterans' sensitive information must prevent unauthorized and unintended information transfer via shared information device resources.

Access to VA Information and VA Information Systems

Question	Response: (Select One)		Comment
	YES	NO	
1. Do you maintain a current list of employees/sub-contractors that are accessing VA's information and information systems for this contract?	☐	☐	
2. Have the appropriate background investigative requirements been met for all employees and subcontractors?	☐	☐	
3. Has access (both technical and physical) to VA information and/or VA information systems been provided to employees and subcontractors, only to the extent necessary to perform the services specified in the contract?	☐	☐	
4. When employees/subcontractors leave or are reassigned, is the contracting officer 's technical representative COTR notified?	☐	☐	

Custodial Requirements

Question	Response: (Select One)		Comment
	YES	NO	
1. Were you required to sign a Business Associate Agreement prior to receiving access to Veterans' sensitive information?	☐	☐	
2. Is Veterans' senstive information, made available by the VA for the performance of this contract, used only for those purposes, unless prior written agreement from the contracitng officer?	☐	☐	
3. Is Veterans' senstive information maintained separately and not co-mingled with any other data on the contractors/subcontractors systems/media storage systems ?	☐	☐	
4. Are you ensuring that Veterans' senstive information gathered or created by the contract is not destroyed without prior written approval by the COTR?	☐	☐	
5. Are you aware that making copies of Veterans' senstive information is not permitted, except as necessary to perform efforts in support of as agreed upon by the VA?	☐	☐	
6. Is the protection of Veterans' sensitive information commensurate with the FIPS 199 security categorization?	☐	☐	

Question	Response: (Select One) YES	NO	Comment
7. If hard drives or other removable media contain VA sensitive information, is the data sanitized (three time wipe) consistent with NIST SP 800-88, *Guidelines for Media Sanitization,* and returned to the VA at the end of the contract?	☐	☐	
8. Does the organization sanitize Veterans' sensitive information, both paper and digital, prior to disposal or release for reuse?	☐	☐	
9. Are you identified and authorized to transport Veterans' sensitive information outside of controlled areas?	☐	☐	
10. Are there policies and procedures documented for protecting Veterans' sensitive information during transport?	☐	☐	
11. Is the information device located within an area that minimizes potential damage from physical and environmental hazards?	☐	☐	
12. Is the information device positioned within an area that minimizes the opportunity for unauthorized access?	☐	☐	
13. Does the organization employ appropriate management, operational, and technical information system security controls at alternate work sites?	☐	☐	

Security Incident Investigation

Question	Response: (Select One) YES	NO	Comment
1. Does your company have a security incident reporting process?	☐	☐	
2. Do you and/or your employees know to immediately report a security/privacy incident that involves Veterans' sensitive information to their supervisor?	☐	☐	
3. Does your company know to report a security/privacy incident that involves Veterans' sensitive information to the COTR and the appropriate law enforcement entity, if applicable?	☐	☐	
4. Does the company collect the information concerning the incident (who, how, when, and where) and provide it to the COTR?	☐	☐	

Training

Question	Response: (Select One) YES	NO	Comment
1. Does the organization employ a formal sanctions process for personnel failing to comply with established information security policies and procedures?	☐	☐	

Question	Response: (Select One)		Comment
	YES	NO	
2. Have all contractors/subcontractors signed the VA National Rules of Behavior?	☐	☐	
3. Have all contractors/subcontractors completed the VA approved security training?	☐	☐	
4. Have all contractors/subcontractors completed the VA approved privacy training?	☐	☐	

Appendix A. References

Department of Veterans Affairs

VA Directive 6500, *Information Security Program*.

VA Handbook 6500, Information Security Program

VA Handbook 6500.1 Electronic Media Sanitization

VA Handbook 6500.3 Certification and Accreditation

Federal Information Processing Standards

FIPS 140-2, Security Requirements for Cryptographic Modules

FIPS 190, Guideline for the Use of Advanced Authentication Technology Alternatives.

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

FIPS 201-1, Personal Identity Verification for Federal Employees and Contractors.

National Institute of Standards and Publications

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*.

NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*.

NIST SP 800-73, *Interfaces for Personal Identity Verification (4 parts): 1- End-Point PIV Card Application Namespace, Data Model and Representation, 2- End-Point PIV Card Application Interface, 3- End-Point PIV Client Application Programming Interface, 4- The PIV Transitional Data Model and Interfaces*.

NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification*.

NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*.

NIST SP 800-88, *Guidelines for Media Sanitization*.