Cyber security policy research paper example

Business, Management

Project 3

Introduction

The completion of this System Security Plan is part of Department of Veterans Affair's operational requirement in accordance to the Federal Information Security Management Act or otherwise Public Law107-347 and the Management of Federal Information Resources. The Veterans Affairs is classified as a Federal Agency, thus requiring the organization to ensure that all computer systems including the sensitive information are ensured of its security and privacy, which justifies the preparation and implementation of this plan. This encompasses an objective of improving the level of protection of all information and IT resources utilized by VA through system security planning. It is mandated that all Federal agencies including the Veterans Affairs are required to implement a level of sensitivity to all critical information held by the agency by means of best management practices and to be documented using a system security plan.

SYSTEM IDENTIFICATION/SCOPE OF Assessment

System Name/Title/Unique Identifier

- System Name: Cyber Security

Security Categorization – It is the process carried out by either the steward or owner of the information system together with the cooperation of the organizations key officials. The process is conducted as an organization-wide activity that considers the overall security system infrastructure of the organization. Often the organization may consider segmenting the system into several subsystems to effectively and efficiently allocate appropriate

security controls.

Information System Type – For VA, once of the most critical information system type that needs to be secured is the Transaction Processing System or TPS. The system captures, process and generates data for the organization on a daily basis. The majority of the staff usually performs activities associated to recording of veterans loan applications, record updates, claims clearing, printing schedules and generally activities that involves data maintenance.

Scope of Assessment – The scope of assessment includes identifying risks to system resources in three key areas such as Technical, Operational and Management control.

- Management CONTROL – Several risks involved and identified in management control are the lack of authorization to expedite critical transactions, weakness in real-time update on information that is highly important in the operations.

Selected Control – Risk Assessment and Authorization is the selected control for this area, identified as CA. It is described as a baseline for monitoring and assessment of authorization levels.

Family Control #RA1 – The organization disseminates, reviews and update policies and procedures that are required to effectively implement risk management strategies.

Implementation Status: Currently a mandatory standard as a response to FISMA.

Implementation of Control: The Veterans affairs will implement management control in terms of closely monitoring the changes that occurs in the system

and determine data sectors that are considered inefficient. In return, the security system will point out the anomalies in the network activities that hinder the effective delivery of VA services including abnormal network traffic volume of transactions. The control mechanism on the other hand will initiate authorization schemes in accordance to the management policies and procedures.

Family Control #RA2 – VA will categorize the stored, processed and transmitted information of the system in compliance to FIPS 199. In addition categorization will also document the results from the system security plan. The high-level organization officials will be designated to approve the categorization if high, medium or low.

Implementation Status: VA will develop and implement security plans that will address security requirement ensuring that the security controls meet the requirements.

Implementation of Control: Each of the categorized information in the system will be evaluated according to the results of the security plan. The level of risk as being high or low will be determined and approved by the VA officials to address improvement requirements.

Family Control #RA5 – Using appropriate techniques and scanning tools, VA’s information system will be scanned for vulnerabilities at least twice a year or when apparent vulnerabilities were reported and identified. The level of control required for this section is from medium to high.

Implementation Status: VA will conduct an assessment to determine impact of vulnerabilities to information privacy in accordance to the policies outlined by OMB.

Implementation of Control: The organization will conduct a semi-annual system scanning of outdated security protocols or if there were instances of anomalous behavior in the system. This way the organization would be able to easily determine the problem and isolate them to avoid the compromising the entire system.

- Technical CONTROL – It generally refers to the implementation of security measures acting as a technical safeguards that prevents harm from being inflicted to the system while imposing confidentiality, system integrity and access availability.

Selected Control – Access control identified, as AC under the technical class will be used for the technical aspects of system security on technical control. This includes protecting system communication and segregation configuring the users, access to resources and source.

Family Control #IA2 – The system is configured to identify users and provide access authorization to information resources stored in the system.

Implementation Status: The organization will manage user accounts placing levels of access depending on information provided by the user to the system. This also includes, activation, modification and removal of user accounts in the system.

Implementation of Control: VA will designate user login to the system in every workstation. The restriction level will depend on the authority provided to the user and each data sector is encrypted and is configured to provide access only when the required user information was correctly keyed in.

Family Control #IA-4 – This security control was designed to identify users according to the information provided to the authenticating tool. The system

verifies the information and matches them to the stored identity modules stored in the system to ensure that only authorized users would be able to gain access to the restricted data.

Implementation Status: Organizations are required to employ automated mechanisms that will manage account creation, modifications and terminations to be audited and notify officials on instances of failed or forced access.

Implementation of Control: VA web and intranet applications are equipped with user login system to ensure that only the authorized users would be able to gain access to the information stored in the system. The management will issue login information to user and the authenticator tool will determine access validity.

Family Control #IA-7

Implementation Status: Executive order, applicable laws, policies and directives to ensure that maximum user sensitivity of the information particularly in Federal agencies such as the Veterans Affairs employ cryptographic modules as authentication tools prescribed.

Implementation of Control: The authentication module for VA staff and member's user logins are encrypted in the system to prevent intruding traffic from picking up user details from the system.

- Operational CONTROL – Defined as countermeasures implemented in the security controls that ate being used and executed by people as per FIPS 200.

Selected Control – Personnel Security, it is a formal security policy that addresses roles, scope, responsibilities, commitment, and management,

coordination associated to personnel control. Procedures are documented before facilitating implementation.

Family Control #PS-2 – The organization itself designates risks to all positions and provides a screening criteria in filling the positions.

Implementation Status: Designations according to imminent risk in personnel's position should be aligned with the directives of the Office of Management Policy including training, clearance and security guidelines

Implementation of Control: VA is tasked to delegate responsibilities, which spreads the amount of risk according to the responsibilities outline in each of the people in the agency.

Family Control #PS-3 - It is a formal security policy that addresses roles, scope, responsibilities, commitment, and management, coordination associated to personnel control. It provides a bigger picture of the conditions and frequency of personal access in the system.

Implementation Status: Individuals are being rescreened for compliance to the organization-defined conditions.

Implementation of Control: The administration department of the VA will ensure that all staff is indoctrinated prior to providing access to sensitive information in the system. Therefore, ensuring that the staff are well screened and passes the screening process to continue accessing the classified information in the system.

Family Control #PS-4 – Retaining access to the information stored in the system by previously terminated personnel will be blocked and the user information will be disabled in the system.

Implementation Status: Exit interviews require that the terminated personnel are made clear of the security constraints of their separation from the organization.

Implementation of Control: It is recommended by the VA administration that all terminated personnel be removed of their access to hardware and software resources of the organization. Exit interviews and clearance procedures will be imposed to ensure that information delegated to the terminated personnel are returned and accounted for.

- CONCLUSIONS/RECOMMENDATIONS – System security plan is an essential step for organizations such as the Veterans Affairs to efficiently execute maximum system security protocols to protect the system infrastructure of the organization. Following the directives stipulated in NIST SP 800-53 ensures that the organization is in the right direction in terms of protecting its information system architecture. Several vulnerabilities are eminent in the cyber environment and the best that the organization can do is to follow the guidelines set in the NIST SP 800-53 publication. Control measures discussed herewith provide a solid ground for VA’s information system security by applying the control procedures identified in management, technical and operational controls.

- Results of Assessment – Based on the information obtained regarding the different control measures, it can be concluded that VA was able to successful comply with all the described procedures in the NIST SP 800-53 guidelines

Recommendations – Veterans Affairs on the other hand should be able to further improve its information security system by means of adapting more

control measures described in the aforementioned publications such as:

- Error handling by complying to the SI-11b Parameter Requirements
- Spam protection to be enabled across all users including website subscribers
- Improving security alerts and advisories
- Malicious code protection, and
- Flaw remidiation

References

Eustace, K. D. (2008). Transforming IA Certification and Accreditation across the National Security Community. Office of the Assistant Secretary of Defense for Networks and Information Integration, Washington DC.

Eustace, K. D. (2008). Transforming IA Certification and Accreditation across the National Security Community. Ft. Belvoir: Defense Technical Information Center.

United States. Joint Task Force Transformation Initiative (2009). Recommended security controls for federal information systems and organizations (800-53). Retrieved from U. S. Dept. of Commerce, National Institute of Standards and Technology website: http://csrc. nist. gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010. pdf