Information Resources - Information Security Risk Assessment Reviews

Approved September 25, 2009
Revised June 5, 2013
Next Scheduled Review: June 5, 2016

Supplements TEES Rule 29.01.99.E1

Standard Administrative Procedure Statement
Information security risk assessments are vital procedures for maintaining the security of information resources.

Reason for Standard Administrative Procedure
The purpose of this procedure is to implement a monitoring process which adequately provides management with assurance that the information on which risk assessment assertions are made is correct.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

   1.1 TEES Security Monitoring Team (SMT) will schedule meetings with appropriate personnel from TEES divisions to review their division information security risk assessment(s). Every TEES division will have reviews scheduled on a recurring and rotating basis. The order of these reviews will be predicated on an examination of each division’s annual assessment report and areas of inherent risk (e.g., confidential information, mission critical systems, problematic conditions).

   1.2 Each division will receive an email describing a general outline of the review process prior to the meeting. Divisions will provide SMT personnel with requested information and assistance for the review. This may include assistance in performing an analysis of the division’s information resources. Where beneficial and feasible, these reviews may utilize automated software tools to provide confirmation and/or information regarding the configuration and classification (e.g., contains confidential and/or mission critical data) of the division’s information resources. Such a process will be conducted efficiently and in a reasonable period of time.

   1.3 SMT personnel will answer any questions division personnel have regarding the risk assessment process with the goal of promoting a better understanding and effective use of the ISAAC Risk Assessment process. SMT will seek suggestions that would benefit the division regarding clarifying and improving the risk assessment tool(s) and process.
1.4 Upon completion and analysis of the review, SMT will provide a draft report within approximately five days to the Division Head or designee and to any division personnel designated by the Division Head or designee. After the draft report is delivered to the Division Head, there will be an approximately two week period for discussion and any appropriate modifications to the report. The final report will be provided to the Agency Director, the Division Head or designee, and designated division personnel within approximately three weeks of the conclusion of the review.

Related Statutes, Policies, or Requirements

TEES Rule 29.01.99.E1, Security of Electronic Information Resources

Contact Office
Information Technology Services
(979) 847-8585