

Topical Appraisal:

Security Categorization of Information and Information Systems

September 30, 2012

1.0 Scope

The Security Categorization of Information and Information Systems topical appraisal is performed to ensure that DOE requirements are met. The appraisal will include a review of applicable regulatory standards, the Ames Laboratory Computer Security Program Plan (CSPP), applicable NIST guidance, and DOE directives.

2.0 Dates

The appraisal was performed from 9/24/2012 through 9/28/12.

3.0 Summary Discussion

- Requirements

Ames Laboratory adheres to the requirements and best practices issued in NIST 800-53 Rev. 3 (“Recommended Security Controls for Federal Information Systems and Organizations”), FIPS 199 (“Standards for Security Categorization of Federal Information and Information Systems”), and the Ames Laboratory CSPP (“Cyber Security Program Plan”).

- Program Documentation

- NIST 800-53 Rev. 3 – Appendix D, Security Control Baselines (Moderate)
- FIPS 199
- Ames Laboratory CSPP

- Training

On the job training is provided to employees as needed.

- Performance

- Review FIPS 199 regarding security categorization.
 - FIPS 199 was reviewed.
- Review NIST documents related to FIPS 199 categorization.
 - NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories was reviewed.
- Review DOE policy and procedures.
 - There are two DOE orders relevant to Information Management and Cyber Security:
 - DOE 200.1A, Information Technology Management.
 - DOE O 205.1B, Department of Energy Cyber Security Program.
 - DOE 200.1A references DOE O 205.1B. DOE O205.1B references FIPS 199.

- Compare these documents against Ames Laboratory Cyber Security Program Plan and associated policies and procedures.
 - The FIPS, NIST and DOE documents were compared.
- Identify discrepancies and create corrective action plan.
 - No discrepancies occurred.
- Review progress of moderate boundary migration.
 - The moderate boundary migration for the administrative offices is complete.
 - The moderate boundary migration for the research programs is in progress.
- Create corrective action plan for overlooked systems.
 - A Maximo Service Request is created when overlooked systems are identified.
 - Once the system is moved to the moderate enclave, the Maximo Service Request status is changed to 'resolved'.
- Conclusions
 - Ames Laboratory was determined to have two Enclaves, Low and Moderate.
 - The sensitivity rating on the Low Enclave for Confidentiality/Integrity/Availability is Low/Low/Low.
 - The sensitivity rating on the Moderate Enclave for Confidentiality/Integrity/Availability is Moderate/Moderate/Low.
 - The security categories were reviewed for potential impact on the Enclaves.
 - The current security categorizations are appropriate for the two Enclaves.
 - The most recent Certification and Accreditation (C&A) review confirmed two Enclaves were adequate and met the FIPS, NIST and DOE criteria.

4.0 References

- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems.
- NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories.
- DOE 200.1A, Information Technology Management.
- DOE O 205.1B, Department of Energy Cyber Security Program.

5.0 Personnel Interviewed

- Kurt Hulsebus
- Mark Clarridge
- Bill Sears
- Diane Den Adel

6.0 Assessment Results

- Strengths
 - No discrepancies were identified.
 - The Authorizing Official acknowledged and approved the current enclave structure including security categorizations.

- Noteworthy Practices
 - Regular configuration management and continuous monitoring meetings occur to discuss low and moderate issues.
 - Maximo Service Requests provide a mechanism for tracking these issues.

- Findings
 - Effort to move the appropriate research groups to the moderate enclave needs to be accelerated.

7.0 Attachments

- None.

A copy of this report will be filed and saved in G:\cyber\topical Appraisals\2012.