Civilian CASE STUDY

National Archives and Records Administration (NARA), Information Technology Security Support

- **Cybersecurity and Information Assurance**
- **Systems and Technical Services**
- **Business and IT Training**

Client Challenge

Implementing robust, enterprise-wide IT Security across the Agency enabling effective business operations.

XLA Excellence Delivered

Since August 2012, XLA has provided Information Technology (IT) security technical support across 11 task areas for NARA's Enterprise infrastructure. We assist NARA leadership with the development and updating of policies and standards, operations with the analysis and proper implementation of security mechanisms and technical aspects by monitoring and reporting on security compliance within the NARA Enterprise. The 11 tasks include:

- **Policy and Guidance.** XLA supports NARA to review, update, develop, and report on Enterprise Architecture Compliance, Security Program Planning, and IT Security Program Evaluation Reporting.
- **Security Awareness and Training Support.** XLA collaborates with NARA to review, update, design, test, and deliver customized training including Tier I, IT Security and Personally Identifiable Information (PII) Awareness Computer Based Training (CBT). XLA also tracks and reports on NARA User completion rates and compliance.
- **Risk Management Support.** We support NARA's Risk Management Framework for tracking IT systems throughout their System Development Life Cycle (SDLC). XLA maintains a Risk Management Framework (RMF) dashboard on a continuous basis, giving NARA management the capability to make decisions from system through enterprise-level risk postures.
- **Security Engineering Support.** XLA provides research and recommendations on security mechanisms for new technologies being evaluated or introduced at NARA. The information XLA gathers as part of the security engineering review is incorporated into packages for project review boards as well as in support of accreditation packages. XLA has also developed tools to assist NARA with responding to and tracking Einstein 3a (E3A) alerts.
- **System Authorization and Reauthorization Support.** XLA performs technical analysis of data from tools used for security scanning, conducts manual reviews of system configurations and system documentation, and interviews system stakeholders to evaluate management, operational and technical controls for optimum security operations.
- **Security Assessment and Authorization for New Systems.** XLA plans and conducts security assessments in compliance with National Institute of Standards (NIST) Special Publication (SP) 800-37 and 800-53a for all new NARA systems meeting Office of Management & Budget (OMB) Circular A-130 and Federal Information Security Management Act (FISMA) requirements.
- **Ongoing Authorization Support.** XLA develops NARA's Annual Assessment Plan used to schedule and conduct the continuous security assessments for all FISMA reportable systems.
- **Continuous Monitoring Support.** XLA developed NARA's Continuous Monitoring Concept of Operations (CONOPS) which specifies security tools in use at NARA, their outputs and their respective reporting frequencies. XLA develops and maintains a Vulnerability and Patch Management Dashboard, enabling NARA's Chief Information Security Officer (CISO) visibility into current risks to agency systems. We also work with NARA System Owners (SOs), Information Security System Owners (ISSOs) and the IT Security Division to create, update and revise Plan of Actions and Milestones (POA&M) elements for NARA information systems to accurately reflect current status of system POA&Ms.
- **Intrusion Detection & Incident Response Support.** We support most incident handling activities at NARA and the methodology for Incident Response by identifying the cause, determining the level of exposure, containing the risk and reporting our findings.
- **IT Security Tool Support.** XLA provides support for all NARA security tools. XLA also provides recommendations to NARA, regarding which tools to use as well as defining best use strategies.
- **Response to Audit Support.** XLA supports security audits or other assessments of NARA's Information Assurance program.

Impact

- Developed computer-based security awareness training that included instruction on NARA's cloud-based email solution, Gmail and PII. The intuitive, easy-to-navigate class led to NARA achieving a 90% completion rate of required annual security training on the first try.
- Using results of our analyses documented in multiple white papers, NARA has removed or reduced redundant systems, thereby lowering costs and the level of effort required by 50% for supporting systems.
- Significantly updated system POA&Ms, giving the CISO a clearer picture of the risks associated with each system.
- Reduced the level of effort by several weeks for completing of assessment activities while maintaining acceptable levels of risk. We achieved this by scanning a sampling of IT assets based on their risk to the enterprise, instead of scanning all assets.
- Developed Risk Management Framework dashboard, enabling Executive Staff to view risks across their enterprise for proper decsonmakingand resource allocation.