FY 2007 E-GOVERNMENT ACT REPORT

FINAL

SEPTEMBER 2007

1. Agency-Specific E-Government Initiative: USAID's Vulnerability Management Program

CISO Security Objective and Vision

The U.S. Agency for International Development (USAID) is an independent federal government agency that receives overall foreign policy guidance from the Secretary of State. USAID's work supports long-term and equitable economic growth and advances U.S. foreign policy objectives by supporting: economic growth, agriculture and trade; global health; and, democracy, conflict prevention and humanitarian assistance. USAID provides assistance in four regions of the world: Sub-Saharan Africa; Asia and the Near East; Latin America and the Caribbean, and; Europe and Eurasia.

The USAID Chief Information Security Office (CISO) is responsible for the development and management of a risk-based Information System Security Program for the agency. The CISO defines security policy, audits risks to the network, provides security awareness training, monitors network security events, and responds to security incidents. Measuring risk is not helpful to the business unless the CISO shares the assessment results with the business owners. Therefore the CISO implemented a vulnerability management solution to audit agency networked systems and evaluate the overall risk of those systems to the cognizant business owner.

Security Communication Strategy

To accurately measure the effectiveness of the security patching process, the CISO needed a tool that could (a) perform the measurements and (b) communicate the resulting measurements to the business and system owners. Through these means, the CISO aimed to empower the business and system owners to make informed, risk-based decisions. For example, each mission (overseas location) has a System Manager who is responsible for their patching process and reports to a system owner. Through the vulnerability management program, the CISO planned to drive patch process refinement by increasing the visibility of system risk posture to the appropriate levels within the agency. The CISO did this through a monthly grading process that communicated risk posture to all levels of the agency without relying on the technical details of the data. The CISO developed a grading system to help communicate the vulnerability level to both the system business owners as well as the technical staff responsible for patching and configuring the systems.

DEPLOYMENT OF SECURITY TECHNOLOGY OR PROCESS

USAID's CISO evaluated several leading vulnerability scanning technologies based upon ease of management, granularity of user access control, scan accuracy, and reporting. The selected tool, nCircle's IP360 Vulnerability Management System, proved to be the perfect solution with which to develop an easily communicated grading system. The IP360 does not use the standard "High, Medium, and Low" severity ratings for vulnerability. Rather, it assigns an integer score to each vulnerability score based on how long a vulnerability has been publicly known, the risk the vulnerability poses to the system, and the skill level required to exploit the vulnerability: The higher the score, the more critical the vulnerability. The score for a host is the sum total of all the vulnerabilities found on the system, while the score for a network of hosts is the average of all the host scores. When System Managers view a report, the systems with the worst host scores rise to the top of the list, showing them instantly where their remediation efforts will make the most impact.

From the IP360 audit data, the CISO engineered a simple grading scale which was easy to understand from a technical or managerial perspective. It was also scalable in its effective application, from the smallest network to the entire enterprise. The team used two figures which are produced by every nCircle network scan for the foundation for their grading scale: the Average Host Score and the Worst Host Score. The grading scale ranges from A to F and includes minuses but no pluses. If the Average Host Score for the network falls within a specified range, it receives a base grade, such as a B. After determining the base grade, the Worst Host Score is compared to the letter grade's Worst Host Score Limit. If the Worst Host Score for the network exceeds the limit, a minus is appended to the grade, making it a B-. In this manner, large networks with one very vulnerable system are not overly penalized.

The IP360 scans the USAID network continually. During the grading period, which runs from the 1st to the 21st of every month, each network is scanned multiple times. System Managers can view the security status of their systems at any time using a web reporting tool. Through this tool they are also provided with detailed scan data for their network, remediation information on each discovered vulnerability, and the differences between this month's report and last month's. On the 4th Tuesday of each month, the ISSO team sends the grade for each network to the responsible system owner, Information System Security Officer (ISSO), and System Manager. The last week of the month is reserved for remediation activities and signature updates on the IP360.

INCREASED SECURITY EFFECTIVENESS

The CISO vulnerability management solution has dramatically changed the way USAID deploys new systems and manages the systems already in service. As a result of the increased visibility into what systems are on the network, the CISO can also use the data to assist with incident response, inventory tracking, configuration management, and change control operations. System Managers now build and patch systems on segregated networks rather than on the production network, and there is a heightened awareness about security. System Managers now know that the scanner may catch them if they place and unpatched system on the network and, therefore have put in place better system deployment processes.

The CISO had planned to wait several months after deployment to disclose the grades to the Bureau heads (global regional directors). This changed when, within one month of the program, the directors learned that the CISO office was grading their missions and requested the CISO provide them with their grades. Even though the Bureau heads did not understand the technical details of specific vulnerabilities at their missions, they could tell the difference between an A and a B. Consequently, they demanded that their technical staff do everything necessary to merit an A.

INCREASED SECURITY EFFICIENCY

Centralized vulnerability management and reporting has ensured accountability and visibility of systems risk levels. This visibility enables the CISO to track the progress and effectiveness of patches processes at a number of different levels: by mission, by region, and as an enterprise.

Providing prioritized, actionable data to System Managers enables them to make the best use of their limited amount of time and to see the immediate impacts of their efforts. It has also proved to be cost-effective to run the systems centrally, rather than at each site or mission.

SECURITY METRICS APPLICATIONS

nCircle provides vulnerability data by system as an integer score. The CISO converts this score into a letter grade by mission (responsible system owner). Immediately, the CISO has a variety of metrics data available for tracking the overall risk posture of the agency and its global sites. For many sites, they now evaluate System Manager annual performance by whether the administrator was able to maintain an A average for the year. The CISO tracks these grades, as an enterprise and by site, from month to month.

In December of 2004, USAID was called upon to provide relief in countries that were devastated by the tsunami. The enormous scale of this disaster required that USAID missions in the region rapidly add staff and computers to support the long-term rebuilding efforts. For example, the USAID mission in Sri Lanka, one of the hardest hit areas, added dozens of new computers to the USAID network. USAID system administration staff worked around the clock to provide the information systems infrastructure to support the United States government relief efforts. Other USAID missions in the affected areas also needed to increase the number of workstations on their networks as well. The unplanned increase in the number of systems connected to the network introduced additional risk to the network. Because USAID continually measures the system risks to its enterprise through vulnerability management, the business was able to make an informed and rational decision to allow this rapid, unplanned expansion of AIDNET and accept the added risk in order to meet the emergency business requirements. Further, USAID could report and track this risk until mitigated to an acceptable level.

Before the risk-based program that nCircle supports, USAID would not have been able to determine the amount of additional risk it was assuming given similar circumstances. The agency did not have monitoring capabilities on its network. Further, USAID lacked an understanding of system vulnerabilities and how they changed its risk. Since that time, the USAID CISO has developed an information security program that leverages vulnerability management technology to address security shortcomings. This empowers the agency to fulfill its obligations to its business owners, ensure compliance with federal standards, and effectively manage the security of its systems and network.

VALUABLE LESSON

The most valuable lesson the CISO learned implementing the vulnerability management program is that measuring the process is the most effective thing an organization can do to ensure that it is staying on top of vulnerabilities. By reporting on these metrics to key stakeholders, the CISO increases the visibility of the process and whatever problems might exist. This increased visibility has fostered better processes and greater security awareness in general.

ONGOING DIALOGUE WITH EXTERNAL AND INTERNAL STAKEHOLDERS

To promote internal dialogue, the CISO holds a weekly Security Working Group conference call. It is a forum that keeps security personnel engaged with current security issues at the agency. The participants discuss broad themes, issues that have potential to become more severe, current investigations, and patching issues. Additionally, a representative from the CISO participates in USAID's Change Control Board to dialogue with IT decision maker in the agency about setting up standards, proposed acquisitions, and other changes to the agency's IT systems.

To stay engaged with industry and external government stakeholders, CISO staff have presented at several security technology conferences, such as the annual RSA Conference and CSI. Such venues allow USAID to demonstrate its technology and learn about the tools that other groups are using. The CISO is also active in the GFIRST community, the Government Forum of Incident Responders and Security Teams sponsored by US-CERT, part of the Department of Homeland Security. USAID's CISO regularly communicates with State Department security personnel about best practices and how to work together effectively.

EXPECTED NEXT STEPS

The CISO has already taken the next logical step in understanding agency risk by integrating the valuable vulnerability data nCircle provides with an enterprise risk management tool from Skybox Security. This technology couples nCircle's vulnerability data for all the agency's network systems with routing and access control data and provides a real time model of the agency's system exposure (and thereby risk) to identified threat sources (such as the Internet). Since Skybox understands the agency's access controls and vulnerability data, it can identify what systems are directly or indirectly accessible to attack based on their true vulnerabilities and access. As a result, the CISO can now provide more detailed information to business owners that can differentiate between, for example, a vulnerable web server that is accessible from the Internet and one that is on an internal network behind several layers of firewalls. They both may have the same vulnerability, but the one that is most exposed to a threat (the Internet in this case) is the one most at risk.

By measuring risk and producing actionable reports, the CISO better secures USAID and its network. Because its network is more secure, USAID avoids the costs associated with incident response, incident repairs, and remediation of exploited systems.

2. Agency Information Management Activities

A. IRM Strategic Plan

USAID is updating and refining its Information Resources Management (IRM) Strategic Plan.

B. Information Dissemination

USAID's information dissemination product catalogues, directories, inventories, priorities, schedules, and management tools used to improve the dissemination of and access to USAID's information by the public:

- http://www.usaid.gov/policy/egov/inventory.html

C. USAID FOIA Requests

- FOIA handbook: http://www.usaid.gov/about/foia/handbook.html
- Primary FOIA Website: http://www.usaid.gov/about/foia/
- Frequent requests for records: http://www.usaid.gov/about/foia/webfreq.html

D. R&D Activities

USAID does not fund Federal R&D activities. USAID's mission focuses on international development, empowerment of nations, and promoting democracy and prosperity in the world. While USAID performs research towards those ends, it does not perform or fund "R&D activities."

E. Information Dissemination: Formal Agreements

USAID does not have formal agency agreements with external entities complementing the agency's information dissemination program. However, in addition to disseminating information through its own website, USAID and its partners maintain many websites dedicated to disseminating USAID mission-related information to communities of practice, communities of interest, NGOs, and the general public. The following is a link to a list of those websites:

- http://www.usaid.gov/policy/egov/usaid_portals_projects.pdf

F. NARA-APPROVED RECORDS SCHEDULES:

Inventory of NARA-Approved Records Schedules:

- USAID Disposition Schedule for E-records: http://www.usaid.gov/policy/ads/500/502maa.pdf: this policy is consistent with NARA General Records Schedule 20, and includes USAID policy on the retention schedule for different kinds of electronic documents.
- USAID Disposition Schedule for paper records: http://www.usaid.gov/policy/ads/500/502mac/502mac_toc.html#2: this policy is consistent with NARA guidance, and includes USAID policy on the retention schedule for different kinds of paper documents.

USAID's progress to implement NARA Bulletin 2006-02:

- USAID identified 46 systems , and provided the inventory to NARA in FY07:
  - 6 systems have been scheduled:
    - Development Experience Clearinghouse NI-286-86-3
    - Agency Full Time Equivalency Report System NI-286-86-3
    - Agency Correspondence Tracking System NI-286-99-1
    - American Employee Time and Attendance System GRS 2
    - Telephone Directory NI-286-99-2
    - Agency Notices NI-286-00-1
  - 40 systems had not been scheduled (as of the end of FY07)
    - See attached Excel Spreadsheet "USAID_E-records_Inventory for NARA scheduling 9-18-07.xls" for complete list.
  - USAID has one system, Documentum: Agency Secure Image and Storage Tracking (ASIST), which is scheduled for internal review and approval before submission to NARA.