March 22, 2016

To: Federal Co-Chair
ARC Executive Director
ARC General Counsel
ARC Director of Finance & Administration

From: Hubert Sparks, Inspector General

Subject: Report 16-11; IT Security Evaluation HS

The attached report was prepared by the International Trade Commission OIG who performed the evaluations in accordance with an agreement with our office.

The evaluations reflect overall ARC implementation of information security measures and the noted recommendations are being addressed by ARC.

Table of Contents

Results of Evaluation

The purpose of this evaluation was to answer the question:

Does the ARC continuously diagnose and mitigate threats to its network systems?

No. The ARC does not continuously diagnose and mitigate threats to its network systems. While ARC employs a process to remedy vulnerabilities on its systems, it does not have the means to continuously identify and remediate vulnerabilities.

Since the last review, ARC has made some progress towards securing its network. The vulnerability scan we performed on November 23, 2015 identified that 30 of 86 measured systems had two or less high-severity vulnerabilities. While zero is the goal for high-severity vulnerabilities, two is an achievable target given the dynamic nature of a network.

The system administrator described that ARC is now configuring its systems to have a common baseline configuration. This is a great practice because it increases security by reducing complexity and it enables efficient maintenance of these systems in the future.

Our analysis of the vulnerability scan of the ARC network produced the following information:

	Hosts found:
Total:	111
Printers:	20
Hosts failing scan:	5
Hosts fully scanned:	86
Average High vulnerabilities per host:	169.9

Top 5 Most Vulnerable hosts:	Vulnerabilities:
192.168.1.138	1671
192.168.1.45	1246
192.168.1.116	736
192.168.1.137	696
192.168.1.153	626

	Total High Vulnerabilities:	Per host
All:	14,624	170
Microsoft:	733	9
Third party:	13,891	162
Adobe:	8,460	98
Firefox	2,802	33
Java	1,541	18

This evaluation identified three problem areas placing the ARC network at significant risk: (1) No tool to assess network for vulnerabilities; (2) Users can run and install unapproved software; and (3) Some systems have an extremely high number of vulnerabilities. These problem areas will be discussed in detail in the rest of this report.

Problem Areas

Problem Area 1:
No tool to assess network for vulnerabilities.

As found in the previous evaluation in 2013, the ARC still does not possess software to monitor the vulnerabilities of its network. Without monitoring, ARC cannot know which of its systems are vulnerable.

Every network today should be monitored continuously for vulnerabilities. Mature, cost-effective software exists to perform this function. This software enables continuous knowledge of the vulnerability status of the network, enabling system administrators to effectively identify and mitigate vulnerabilities.

Without this tool, the system administrator is shooting in the dark to understand and mitigate the risk vulnerable systems present to the network. This increases administrative workload and decreases efficiency, and increases the risk to the network and therefore the ARC organization. No modern network should be without monitoring tools.

Recommendation 1: Acquire and implement a continuous vulnerability scanning tool.

Problem Area 2:
Users can run and install unapproved software.

Only approved software should be installed or allowed to be run on a managed network. At ARC, anyone can run any software application, and many users have local administrator privileges, allowing them to install any software they choose.

This places the ARC at significant risk, primarily from the perspective of being vulnerable to malicious software.

The vulnerability scan performed during this evaluation identified five systems with "WildTangent" software on the ARC network. This software allows the play of games over the Internet, and also gathers and transmits information about the system where it is installed to a third party over the Internet. ARC should carefully review and limit the transmission of private network data from disclosure to third parties.

Effective software risk management requires the implementation of two controls:

1. Limit administrative privileges.
2. Whitelist (allow) only approved applications.

Vulnerability scanning software can quickly identify all administrative privileges on the network, and the system administrator can then edit these permissions to reflect the needs of the ARC.

Whitelisting technology is included and available for no extra cost with the ARC's licensed operating system. The system administrator can immediately configure and activate this software to allow only approved software to run on ARCs network. This method is the most effective one known to control the execution of software on a network of PCs.

Recommendation 2: Grant administrator privileges only to selected individuals that need them.

Recommendation 3: Remove administrator privileges from those users without the need for them.

Recommendation 4: Implement whitelisting control to allow the execution of only authorized software on the network.

Problem Area 3:
Some systems are extremely vulnerable.

Ideally, systems should have zero high-severity vulnerabilities. Only one high-severity vulnerability is needed for a system to be compromised using a widely known, public exploit.

At ARC, systems had on average 170 high-severity vulnerabilities each. Two systems had more than 1000 high-severity vulnerabilities. This happened because ARC does not effectively measure and patch the systems on its network.

Because its systems have so many vulnerabilities, ARC is vulnerable to both drive-by and targeted attacks. These attacks can be triggered by opening an email attachment, visiting a malicious website, or even by simply loading an advertisement on a "safe" website.

Recommendation 5: Set an average target of 2 or less vulnerabilities for all systems on the network.

Recommendation 6: Patch high severity vulnerabilities within 48 hours.

Recommendation 7: Identify and patch the most vulnerable systems immediately.

Recommendation 8: Report average vulnerability data monthly to senior management.

Objective, Scope and Methodology

Objective:

Does the ARC continuously diagnose and mitigate threats to its network systems?

Scope:

The scope of this evaluation included all servers, workstations, and other network equipment providing services and security on ARC network.

Methodology:

1. Used Nessus with current definitions to perform an authenticated scan of all infrastructure and endpoints related to the ARC network.
2. Identified systems that could not be scanned due to technical or policy issues.
3. Analyzed vulnerabilities to remove false positives, and classified findings to identify trends and the causes of unpatched vulnerabilities.