Mr. Charles Coe, Assistant Inspector General
for Information Technology Audits and
Computer Crime Investigations
Office of the Inspector General
U.S. Department of Education
550 12th Street, SW, Suite 8129
Potomac Center Plaza
Washington, DC 20024-6122

Dear Mr. Coe:

Please find enclosed the Nuclear Regulatory Commission (NRC) Office of the Inspector General's (OIG) Assessment of NRC's Efforts to Protect Sensitive Information (OIG-06-A-23).

We conclude from our assessment that NRC's current policies and procedures do not meet the requirements outlined in OMB M-06-16. (b)(7)(E)

(b)(7)(E)

If you, or a member of your staff, have any questions on this matter, please call me at 301-415-5915 or Beth Serepca at 301-415-5911.

Sincerely,

Stephen D. Dingbaum
Assistant Inspector General for Audits

Enclosure: As stated

Bcc: L. Reyes, EDO
M. Johnson, OEDO

(b)(7)(E)

Distribution
(b)(7)(C)

(b)(7)(C)

(b)(7)(C)

~~OFFICIAL FILE COPY~~

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

APPENDIX I: IG DATA COLLECTION INSTRUMENT

Overall Summary Statement. (Please refer to page five of the review guide for sample language for summary statements.)

Based on our evaluation, we found that NRC's current policies and procedures do not meet the requirements outlined in OMB M-06-16. NRC has proposed several actions regarding the protection of PII. These include short-term activities focusing on improving agency staff awareness, reviewing and updating current agency direction to meet OMB's requirements, and assisting offices in identifying current data sources containing PII. Mid-term activities focus on implementing mitigation strategies to protect PII from unauthorized use. Long-term activities include updating agency policy to reflect PII requirements; completing the certification and accreditation of all NRC major systems; and designing, developing, and implementing a uniform Enterprise Security Architecture based upon Federal and commercial "best practices." While NRC has proposed these actions to the Chairman they have not been disseminated to the entire agency. Therefore, there are not adequate controls currently in place to protect PII that is accessed remotely or physically removed from NRC-controlled space.

November 30, 2006

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

FROM: Stephen D. Dingbaum ***/RA/***
Assistant Inspector General for Audits

SUBJECT: SOCIAL ENGINEERING ASSESSMENT (OIG-07-A-04)

This report represents the results of the subject assessment. Agency comments provided at the exit conference on November 8, 2006, have been incorporated, as appropriate, into this report. The agency did not provide formal comments.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG follow up as stated in Management Directive 6.1.

We appreciate the courtesies and cooperation extended to us by members of your staff during the assessment. If you have any questions, please contact me at 415-5915 or Beth Serepca at 415-5911.

Attachment: As stated

ELECTRONIC DISTRIBUTION

John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Janice Dunn Lee, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
William F. Kane, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration and Chief Information Officer, OEDO
Michael R. Johnson, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Cynthia A. Carpenter, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials and Environmental Management Programs
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
R. William Borchardt, Director, Office of New Reactors
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV

EVALUATION REPORT

~~OFFICIAL USE ONLY~~

Social Engineering Assessment

OIG-07-A-04 November 30, 2006

Social Engineering Assessment

Submitted to:

Office of the Inspector General
U.S. Nuclear Regulatory Commission

Final Report

Submitted by:

Systems Research and Applications Corporation

A wholly owned subsidiary of:

SRA International, Inc.
3434 Washington Blvd
Arlington, Virginia 22201

11 November, 2006

Table of Contents

Executive Summary

The SRA International, Inc. (SRA), Social Engineering (SE) Team, at the request of the Nuclear Regulatory Commissions (NRC) Office of the Inspector General (OIG), conducted tests to determine specific weaknesses and vulnerabilities with the NRC's physical, personnel, and network access controls. These tests were designed to simulate social engineering attempts to infiltrate and exploit vulnerabilities on three distinct attack vectors (telephonic, cyber, and physical) within the NRC security infrastructure. The SRA SE Team's tests were designed to be a building block by which the OIG could further assess the NRC security posture and enhance existing controls where necessary.

(b)(7)(F)

(b)(7)(E)

Conclusion and Recommendations

NRC has in general developed strong security programs and practices that, if followed and occasionally tested, will provide barriers to all but the most determined attackers. NRC has also taken measures to ensure that its main information systems are protected against unauthorized access and access attempts. However, the SE Team did find exploitable avenues within the PDR, as well as a weakness in observed Help Desk procedures.

NRC employees demonstrated excellent awareness of IT security responsibilities in their responses to the SE Team's attempts to exploit physical, cyber, and telephonic vulnerabilities. Employees were unresponsive to overt attempts to obtain personal data, and appropriately escalated the perceived incidents to NRC security.

However, the SE Team was able to enter the NRC White Flint 1 and 2 facilities under false names and carry into the facility IT devices that were subsequently used to infiltrate NRC networks and gather intelligence data.

The SE Team's testing indicates that there are areas for improvement. Specifically:

- Help Desk administrators should have controls in place that allow them to validate the identity of callers.
- PDR workstations should employ stronger access controls to limited potential misuse and network disruptions.
- Physical security personnel should be more vigilant and attentive to individuals entering and exiting NRC facilities.

The body of this report contains 10 specific recommendations for improvement in the telephonic, cyber, and physical security areas. Only one vulnerability, SE team's observations of the Help Desk procedures, is of such magnitude to constitute a major finding. Other findings when viewed independently are not major breaches; however, when these are combined, they may provide avenues for malicious activity.

Background

Effective security is multi-faceted. Without the integrated protections provided by the various components of a defense-in-depth strategy, an organization may be vulnerable to threat sources attaining critical business information and sensitive personal data. Recent examples where Federal agency and private corporate data became publicly available highlights the necessity to provide and ensure protections in all areas. Unless agency technical, management, and operational security controls work in concert, there will be opportunities for an attacker to gain access through the weaknesses of the faulty security construct. Accordingly, an organization's security posture is only as strong as its weakest link, which more often than not is the result of human error, lack of knowledge, or misplaced trust.

Social engineers seek to exploit these factors to gain access to facilities and critical information systems and data. They often rely on individuals' lack of knowledge or awareness of security policies and procedures, coupled with a natural tendency to trust other peoples' intentions, in order to build relationships and gradually lay the groundwork for a successful exploit of security mechanisms. Effective user training and widespread awareness of security policy and common security mistakes is critical to effective security program compliance, control, and enforcement. Therefore, it is important for an organization to identify its most critical personnel and operational weaknesses so it may improve the mechanisms through which it delivers its security message to employees. A thorough understanding of various social engineering techniques is paramount to providing proper training and safeguards.

Purpose

The NRC OIG contracted with SRA to conduct an assessment, using basic social engineering techniques, of vulnerabilities and weaknesses in relation to established NRC physical access and network controls. Security testing of this type was conducted to test the adequacy and effectiveness of security control measures and training used to protect the security and integrity of sensitive information technology systems and data. During the social engineering tests, discovered vulnerabilities were exploited by the team.

Scope

(b)(7)(E)

(b)(7)(E)

Results:

Activities, Findings and Recommendations

A. Telephonic Activities

Telephonic testing/intelligence gathering is a common vector for social engineering. Typical targets for telephonic social engineering are help desk administrators, new employees, and entry-level employees. The following is a list of telephonic testing activities conducted by the SE Team, findings as a result of these activities, and recommendations to improve specific weaknesses.

Activity A.1: SE Team members telephoned the NRC Help Desk posing as NRC employees and requested that their passwords be reset.

Major Finding: The SE Team observed that the Help Desk only identifies users by user names, and the individual help desk members were easily manipulated into resetting account passwords. This allowed the SE Team unauthorized access to user e-mail accounts. One solution to this problem is to require the user to provide verifiable information to confirm their identity.

(b)(7)(E)

Finding: After multiple successful calls, the SE Team discovered that all temporary passwords included the word "today" followed by the day of the month (todayXX). Using a static password configuration permits an attacker to attempt a brute force attack against the NRC using combinations of three-character user names and a password of "todayXX."

(b)(7)(E)

Activity A.2: The SE Team entered the NRC PDR and identified several network and telephone jacks under the desk of a PDR workstation.

Finding: An additional point of connectivity (phone jack) was identified, and a visual inspection confirmed that the jack was connected to what appeared to be telephone cable. However, a PDR staff member confronted the SE Team and reported the incident to security before the team could verify its operational status using telephone testing tools.

Finding: An additional point of connectivity (network jack) was identified, and a visual inspection confirmed that the jack was connected to what appeared to be network cable. A laptop was connected and no packets were seen traversing the network port, indicating

that there was no connection to a valid network. If successful, it would appear to NRC employees that calls were originating from an internal source (calls would be identified by caller ID as a 301-415-####), thereby establishing a trust relationship and opening the door for further exploitation.

(b)(7)(E)

Activity A.3: The SE Team made several calls to regional and headquarters employees and blatantly requested user names and passwords, in hopes that employees would report the attempts to the Help Desk and IT Security group. After the calls, the SE Team contacted the Help Desk and posed as the employee that was subject to the attack.

Finding: Although the Help Desk had received multiple calls from employees reporting the incidents, the SE Team observed no attempt to confirm the identity of the caller and immediately reset his/her password. This allowed the SE Team to access the user's account.

(b)(7)(E)

Activity A.4: SE Team members made over 30 telephone calls to NRC employees in all four regions, including headquarters, using different techniques to gain access to usernames and passwords.

Finding: All phone calls attempting to gain user names and passwords directly from NRC employees were denied, and in several cases, our calls were immediately reported to the NRC's regional and local security staff. Therefore, continue NRC IT Security Awareness and Training programs aimed at educating employees about sensitive information.

B. Cyber Activities

The SE Team performed a variety of cyber attack methods in order to identify potential threats and vulnerabilities to NRC information systems, facilities, and employees. The following is a list of cyber activities conducted by the SE Team, findings that accompany these activities, and recommendations to improve these weaknesses.

Activity B.1: The SE Team conducted open source intelligence gathering on NRC Web sites, in order to attain additional information to be used during the attack phase. The team was able to ascertain user names, specific NRC vernacular, and additional exploitable avenues.

Finding: The NRC telephone directory and Office of Human Resources reports are accessible on the NRC Web site. Although this information is considered public record, the level of detail

provided easily allowed the SE Team to develop target profiles, establish credibility, and identify account user names (first, middle, and last initial). The NRC directories provided employee-specific job titles, start dates, departmental offices, office locations, mail stops, and telephone numbers. The SE Team was able to use this information as credible evidence to manipulate employees, security officers, and Help Desk administrators into believing they were actually engaging with the targeted individual. Thus, NRC should ensure that the information provided does not enable hackers to establish particular patterns regarding user names and passwords. For example, removing employees' middle initials from the directory would have prevented the SE Team from being able to distinguish a pattern between employees' initials and user names and would have exponentially increased the difficulty in discerning them.

(b)(7)(E)

Activity B.2: The SE Team was able to access the Internet from PDR workstations.

Finding: The SE Team was able to achieve unrestricted access to the Internet using the NRC PDR workstations. The team was able to access a variety of Internet sites including interactive online diaries, Web logs, known as "blogs" and social networking sites. If NRC elects to allow users access to the Internet, access should be controlled using access control lists called "*whitelists*" to allow access only to approved sites. In considering Internet privileges, NRC should be aware that using the Internet may open the door to NRC prohibited or illegal activities. For example, users may access illegal material, attack another entity outside of the NRC, or post objectionable or malicious content, which would appear to be originating from an NRC IP address.

(b)(7)(E)

Activity B.3: The SE Team was able to use PDR workstations to download common hacking tools from the Internet.

Finding: The SE Team was able to access common "hacking tools" such as Nmap, which is a free port scanning software designed to: detect open ports on a target computer, determine which services are running on those ports, and infer which operating system the computer is running (this is also known as fingerprinting). Accessing this tool from a PDR system enabled the team to look at the other computers on the PDR network

and determine specific vulnerabilities. If NRC elects to allow users access to the Internet, workstations should be locked in "kiosk" mode, which allows only one application to run on the device at a time. In this mode, the user cannot close the application or start another one while kiosk mode is enabled. If a device is reset, the application is restarted automatically, thereby allowing users to only access an Internet browser or the ADAMS system.

Activity B.4: The SE Team successfully downloaded Ollydbg debugger to PDR public workstations, attached it to the Internet monitoring process, and disabled the process.

Finding: The security controls on PDR workstations are susceptible to bypass, which not only puts users of the PDR at risk of losing authentication information, but also increases risks to publicly available systems, such as ADAMS. The ability to access the Internet and install a debugger, a tool typically used by programmers and reverse engineers to identify bugs in software applications, allowed the SE Team to disable the program responsible for controlling system access and subsequently launch executable code otherwise restricted by the host operating system. The debugger was also used to load "cmd.exe" (the Windows command line interpreter) and execute commands that gave the SE Team elevated privileges.

The severity of this finding is increased by the accessibility of the Internet. Internet access combined with access to command line interpreters opens the PDR terminals to more malicious hacking tools such as a "key stroke logger," which records all keystrokes made by users, including usernames, passwords, and other confidential or private information. Malicious attackers with access to PDR workstations could use these tools to compromise the security of the ADAMS system or other systems accessible via the PDR. Although the SE Team did not attempt such attacks, the control gained was more than sufficient to successfully accomplish them. Rather than using the operating system's security features to "hide" unnecessary or dangerous components, the components should be removed entirely from the PDR workstations. For example, removing executables, such as Notepad and the Windows "Help" functions, will reduce risk and prevent exploits from unauthorized or malicious users who can use these programs to bypass security controls.

(b)(7)(E)

Activity B.5: The SE Team brought a personal laptop through security, into the PDR, and connected the laptop to the PDR network (see A.2).

Finding: The SE Team was able to connect to the PDR network and "sniff" traffic with the personal laptop. The team was also able to select an IP address and connect to the Internet using the PDR network. Connecting to the Internet with an unauthorized or

personal computer may introduce a host of vulnerabilities, including malware, viruses, worms, etc. Also, it may allow hackers to easily use common hacking tools to access the NRC network. MAC address locking or 802.1x should be implemented in the PDR as a means to keep unauthorized users off the system, and track what is on the PDR network. Switches should be used to prevent sniffing of user activity.

(b)(7)(E)

Activity B.6: The SE Team tested NRC incident response capabilities with aggressive transmission control protocol (TCP) scanning. TCP scanning is a technique used by hackers to enumerate active hosts and services available on those hosts. Techniques such as TCP scanning and fingerprinting are valuable to attackers because they allow vulnerable systems to be uniquely identified. This allows an attacker to focus efforts on the known vulnerabilities of the systems, ultimately enabling the attacker to facilitate rapid attacks.

Finding: Repeated attacks from the SE Team using TCP scanning resulted in the NRC network becoming permanently unreachable. The NRC's response to our activities indicates that the NRC Incident Response Team follows standard security protocols and immediately blacklists aggressive entities, thereby limiting the effectiveness of attacks using conventional hacking techniques.

Activity B.7: The SE Team attempted to access available applications to identify Cross Site Scripting (XSS). XSS attacks are a family of vulnerabilities which allow an attacker to use a Web server to attack by exploiting trust relationships. The most common example is called "phishing." Phishing e-mails attempt to coerce a user to visit a site, such as a bank or government agency, and manipulate them into divulging confidential information such as user names, passwords, or account information. Should an unsuspecting user follow a link from the e-mail, the attacker can steal credentials stored in a Web browser and use them to authenticate to another system. The SRA SE Team looked for XSS vulnerabilities, in an effort to launch a SPAM (unsolicited e-mail) attack against the NRC user base, using the list of usernames and e-mail addresses previously obtained from the NRC telephone directory and Office of Human Resource reports. These attempts occurred both from the SRA network and the PDR network.

Finding: NRC applications did not appear susceptible to Cross Site Scripting.

Activity B.8: The SE Team attempted to conduct open source intelligence gathering on archived news groups, which often contain useful information such as: access control lists (ACLs), e-mail lists, firewall configurations, vendors, or information about specific operating systems, policies, and procedures.

Finding: No information pertaining to NRC policies or procedures was ascertained after

an exhaustive search of publicly accessible news groups and mail archives. The lack of such information prevented the SE Team from attacking the NRC or bypassing security controls using this vector.

Activity B.9: The SE Team attempted to conduct a phishing attack by using vulnerabilities associated with the Internet Simple Mail Transfer Protocol (SMTP). Typically this is called relaying, which was effective in the early days of the Internet when bandwidth was limited. Today there is little need for mail relaying, although many agencies and corporations still have mail relaying enabled. Considering these potential vulnerabilities, the SE Team attempted to connect to the NRC mail server to send "spoofed" e-mail using SMTP relaying.

Finding: NRC mail servers are adequately configured with anti-spoofing rules and resulted in the immediate termination of SRA's network connectivity, based on the IP source of the attacks.

Activity B.10: The SE Team attempted to conduct a phishing attack by sending an e-mail to specific NRC users, notifying them of the need to complete the required NRC IT Security Awareness and Training course (Illustration 10).

Finding: NRC mail servers effectively blocked the e-mail and terminated network connectivity.

C. Physical Activities

SRA used physical testing to identify potential vulnerabilities to NRC facilities and physical security procedures. The following is a list of physical testing activities conducted by the SE Team, specific findings related to the tests, and recommendations to improve these weaknesses.

Activity C.1: On multiple occasions, the SE Team entered the NRC White Flint 1 and 2 facilities and proceeded through security with a digital camera equipped cell phone. Once inside the PDR, the SRA SE Team was able to take detailed pictures of visitor's badges, room layout, entry points, emergency exits, surveillance cameras, and screenshots of ADAMS documents (See Illustration 12).

Finding: NRC Security Guards do not enforce or notify individuals of established security policies regarding the prohibition of camera equipment within NRC buildings.

(b)(7)(E)

Activity C.2: The SE Team was able to leave NRC headquarters on multiple occasions without returning NRC-issued visitors' badges.

Finding: Security personnel were positioned approximately 10-15 feet away from exit points, thereby preventing them from effectively stopping visitors from exiting the building without completing established exit procedures, particularly during peak business hours. This finding will be followed up by the audit currently being conducted on the badge access system.

Activity C.3: The SE Team signed in to One White Flint and was issued badges on several occasions, despite providing illegible or false information. On two separate occasions, the SE Team member provided a US drivers license but logged in with an illegible name and listed their origin as Iran.

Finding: Security personnel did not thoroughly inspect identification cards or verify visitors' identity prior to allowing building access.

(b)(7)(E)

Activity C.4: The SE Team used basic computer programs to recreate a contractor badge from photographs attained from viewing badges outside of NRC such as at local restaurants. (See Illustration 12)

Finding: The SE Team made a forgery of both the front and back of an NRC badge. This forgery was made possible by personnel leaving their badges clearly visible when outside the buildings either near the NRC facilities or while visiting local commercial establishments. Photographs were easily obtained with cameras and cell phone cameras. The badge was not used in any attempt to gain access. Our observations indicated that with only visual inspections being conducted by the guards we would have gained unchallenged access to the facility. This finding will be followed up by the audit currently being conducted on the badge access system.

Activity C.5: The SE Team approached the NRC White Flint 1 and 2 facilities on foot and attempted access via the east and west car entrances. Each attempt resulted in approaches by armed security personnel who requested identification and questioned at length the nature of their visit.

Finding: External security personnel were very aware of visitors and took necessary precautions to ensure that unauthorized individuals were not able to access restricted areas.

Activity C.6: The SE Teams gained visitor access to One White Flint and proceeded toward Two White Flint to wait at secured stairwells and elevators for employees to enter or exit. Despite attempts to manipulate individuals into allowing access (e.g., talking on the phone, carrying a briefcase and a drink, asking politely, etc.), employees were cognizant of tailgating attempts and did not allow them.

Finding: Employees are aware of physical access restrictions and take necessary precautions to ensure individuals do not gain unauthorized access.

Activity C.7: The SE Team observed an open stairwell in One White Flint and sought to gain access to alternate floors. The stairwell was unguarded, but was monitored by surveillance cameras and contained physical access control devices that prevented further exploration. The NRC should continue to enforce physical restrictions and access controls to facilities.

Finding: The NRC has taken necessary access control measures to ensure that access is restricted to authorized personnel. Elevators and stairwells leading to restricted areas are monitored with surveillance cameras and require badge access.

Activity C.8: The SE Team attempted to gather open source intelligence information by striking up conversations with employees and contractors outside of NRC facilities (smoking areas, benches, and lunch tables).

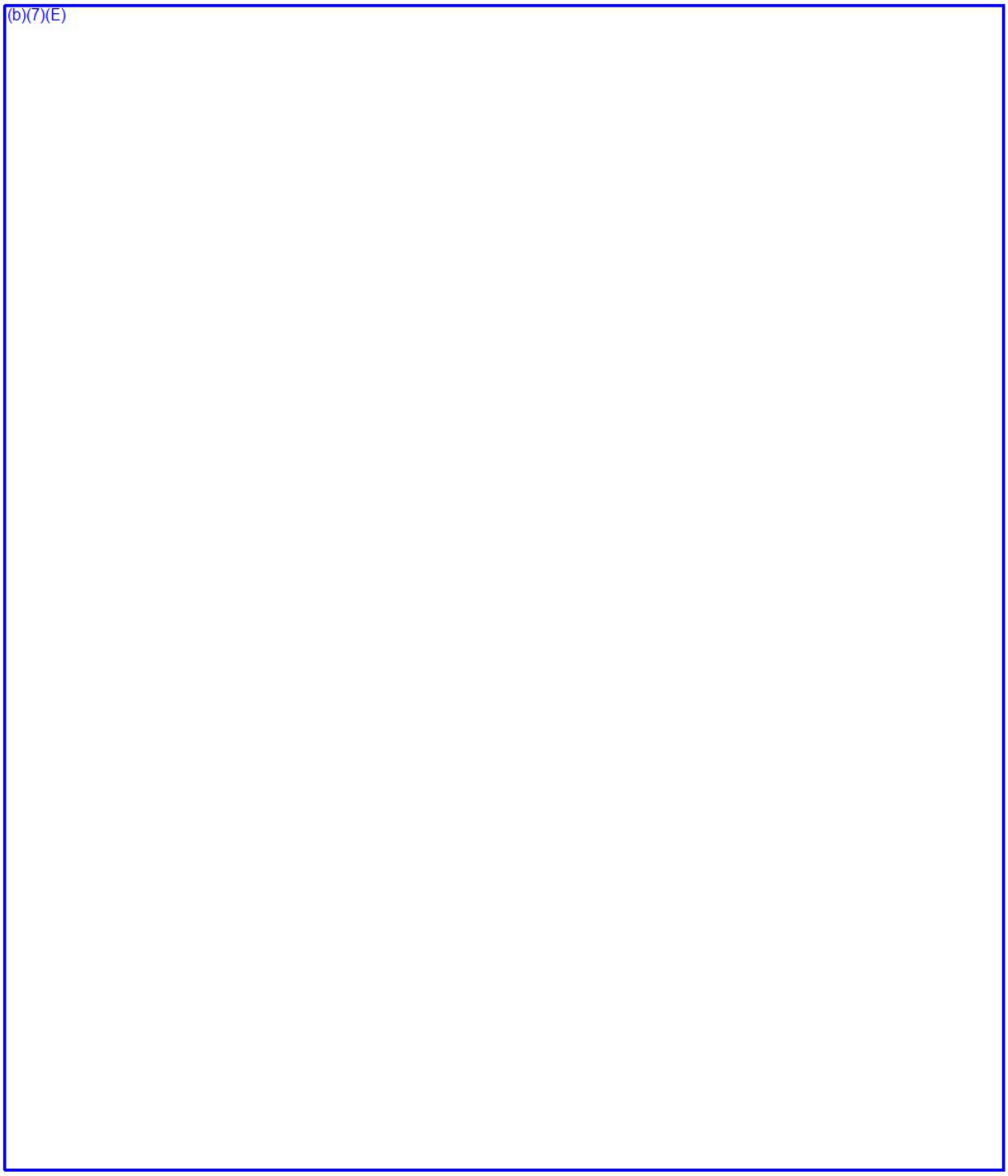
Finding: Employees and contractors, although friendly, were reluctant to discuss the particulars of NRC security, their specific job functions, or other sensitive information. The NRC should continue educating employees on the importance of guarding sensitive information.

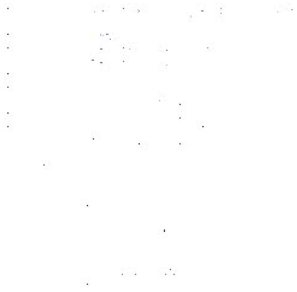
Conclusion

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(7)(E)





Office of Nuclear Reactor Regulation (NRR)
Items of Interest
Week Ending May 19, 2006

Combined Mitigating Systems Performance Index and Reactor Oversight Process Working Group Public Meeting

Pilgrim Nuclear Power Station License Renewal Public Meetings

Staff Issues NUREG-1850 entitled "Frequently Asked Questions on License Renewal of Nuclear Power Reactors"

Final Supplemental Environmental Impact Statement (SEIS) Issued for Nine Mile Point License Renewal

Events in Support of the Expected Vogtle Early Site Permit Application

Department of Energy Publishes Interim Final Standby Support Rule in Federal Register

Byron 1 and Braidwood 2 Sump Modifications

Tennessee Valley Authority Power Uprate Meeting

General Electric (GE) Site Visit Regarding Interim Methods Topical Report Review

Site Audit of the North Anna Early Site Permit Application Dose Calculations

On May 16, 2006, the staff conducted an audit of the dose calculations provided in Revision 6 of Dominion's Early Site Permit application for the North Anna site. During the audit, the staff found errors in General Electric's (GE's) dose calculations for its economic and simplified boiling water reactor (ESBWR) design. The errors included the use of an inappropriate source term for evaluating the consequences of a fuel handling accident as well as mistakes in converting between radiological units of measure. The results of these dose calculations were used by Dominion to justify, in part, the acceptability of the ESBWR as a surrogate design for the North Anna site. Dominion is expected to submit corrected dose calculations and results for the staff's review by May 24, 2006.

Illustration 4: Weekly Items of Interest As illustrated in the highlighted document above, publicly available Commission Documents, such as the SECY reports, provide information that could allow hackers to determine specific weaknesses in NRC

facilities. Information such as this adds to the value of the attack profile, and should not be available to the general public.

Office of Human Resources (HR)
Items of Interest
Week Ending September 1, 2006

Arrival		
ABDEL-KHALIK, SAID I.	ACRS MEMBER	ACRS
ADLER, JAMES E.	LEGAL INTERN	OGC
ALLEN, TAMI T.	HUMAN RESOURCES SPECIALIST	HR
ALLSTON, DENNIS	SECURITY SPECIALIST	NSIR
ARORA, SAM	MECHANICAL ENGINEER	NRR
BARKMAN, MOLLY L.	LEGAL INTERN	OGC
BOLLOCK, DOUGLAS R.	REACTOR ENGINEER	RIV
BROWN, WANDA	SECRETARY (OA)	NSIR
BUDZYNSKI, JOHN T.	REACTOR SYSTEMS ENGINEER	NRR
CHAMBERS, MICHAEL L.	REACTOR ENGINEER	RIV
CORRADINI, MICHAEL L.	ACRS MEMBER	ACRS
CURATOLA, ANDREA L.	LEGAL INTERN	OGC
DICKMAN, PAUL T.	EXECUTIVE ASSISTANT	COMM
DOZIER, TAMSEN S.	PROJECT MANAGER	NRR
GETTYS, EVELYN	PROJECT MANAGER	NRR
KAMMERER, ANN	GEOPHYSICIST	RES
KONOVITZ, LORI S.	CONTRACT POLICY ANALYST	ADM
KORTH, KELLY J.	PROJECT ENGINEER (RI DEVEL. PROGRAM)	RII
LEEDOM, JAMES	CONTRACT MANAGEMENT SPECIALIST (NSPDP)	ADM
LIOTTA, PHILIP L.	HEALTH PHYSICIST	NMSS
MARTIN, JODY C.	LEGAL INTERN	OGC
MEGHANI, VIJAY L.	REACTOR INSPECTOR	RIII
MORRISON, JENNIE L.	HUMAN RESOURCES ASSISTANT	RIV
MURPHY, VICKIE	SECRETARY	RES
OGLESBY, JR., JOHN HAIL	CRIMINAL INVESTIGATOR	OI
PESSIN, ANDREW	ATTORNEY	OGC
PRATT, NICOLE A.	CONTRACT MANAGEMENT SPECIALIST (NSPDP)	ADM
RAJANI, JANAK	IT SPEC (SYS ANALYSIS)	NRR
RICKS, OLIVIA S.	SECRETARY (OA)	NRR

RIVERS, JOSEPH D.	SENIOR LEVEL ADVISOR ON SECURITY	NSIR
STREIT, KATHERINE N.	GENERAL ENGINEER (NSPDP)	NRR
STROSNIDER, SUZANNE D.	IT SPEC (SYS ANALYSIS)	NRR
TANEJA, DINESH	INSTRUMENTATION & CONTROL ENGINEER	RES
TUCCI, CHRISTINE A.	SECRETARY (OA)	NRR
WHALEY, SHEENA	NUCLEAR ENGINEER	NMSS
XIE, BILL J.	CONGRESSIONAL AFFAIRS ASST	OCA
Retirements		
BECKNER, WILLIAM D.	PROG DIR, NEW, RES & TEST REACTORS	NRR
LEACH, ELLA L.	SECRETARY (OA)	OIS
MADEDA, TERRY J.	SR PHYSICAL SECURITY INSP	RIII
RAMMLING, GEORGANNA	FREEDOM OF INFO. & PRIVACY SPECIALIST	OIS
SINGH, AMARJIT	SENIOR RELIABLITY AND RISK ENGINEER	RES
Departures		
BROWN, NICOLE LOIS	STUDENT CLERK	ACRS
DALZELL, JENNIFER L.	STUDENT ENGINEER	RIII
DICKINSON, LYNN ANN	OFFICE SERVICES ASSISTANT	RIV
ENGEL, BETHANY L.	LEGAL INTERN	ASLBP
KALKMAN, ADAM	STUDENT CLERK	OI
Departures		
KING, MONIQUE L.	CONSULTANT	OIG
LEMONCELLI, MAURI T.	ATTORNEY	OGC
PROCTER, CANDACE N.	STUDENT ENGINEER	RIII
VOSS, PATRICIA J.	STUDENT ENGINEER	RIII

Illustration 5: Personnel Lists The Office of Human Resource reports, found in the SECY documents, allow attackers to determine specific targets. This information allowed the SE Team to identify a target by providing us with the user name (based on initials), their job title, and regional office location. The telephone directory provided departmental information that added to the value of the profile.

Compromised PDR Public Workstation

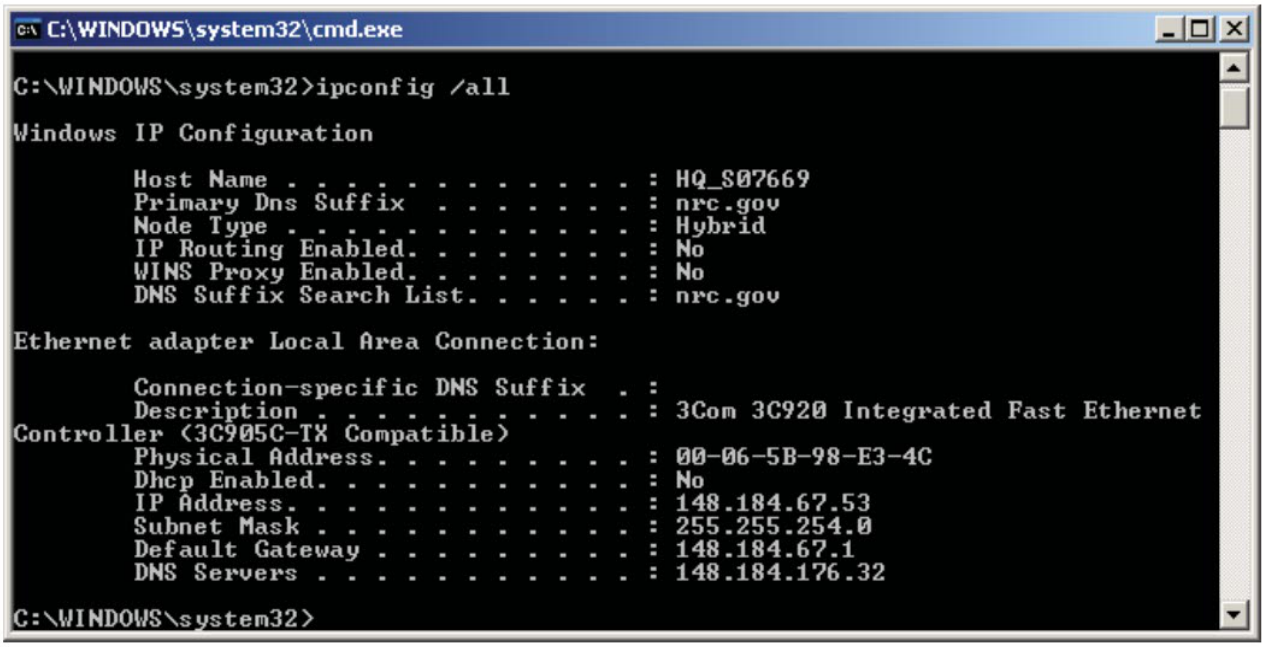


Illustration 6: Command Line access The illustration above is a screen capture demonstrating the SE Team's ability to access the command line interpreter on a PDR workstation. The command line interpreter was inaccessible without the use of the downloaded debugger.

Compromised E-mail Account

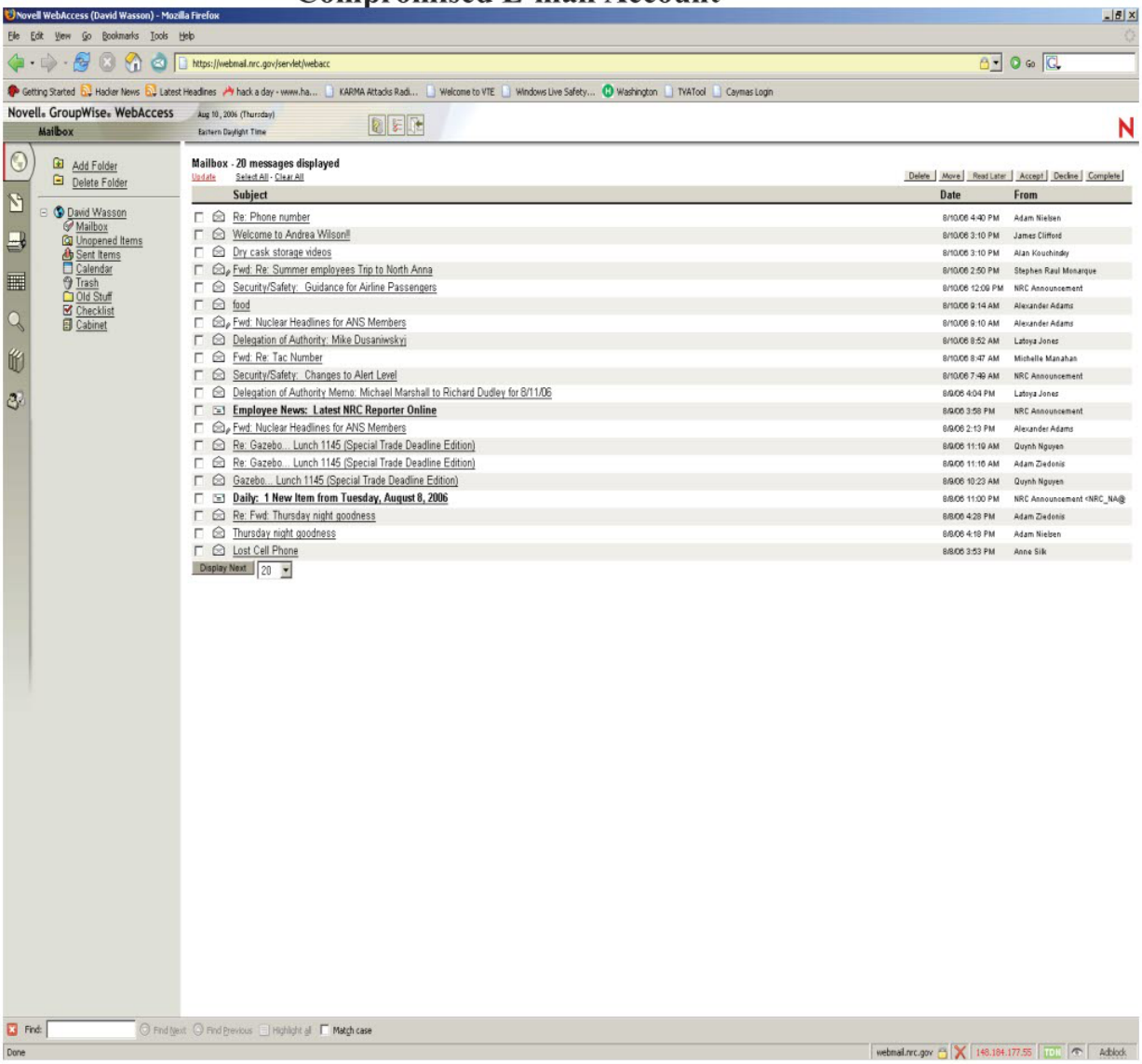


Illustration 7: Compromised account The account illustrated above was accessed through manipulation of the NRC Help Desk. After the SE Team posed as an employee experiencing problems with their remote access capabilities, the administrator reset both the user's remote access and network passwords to a default.

Access to E-mail Alert

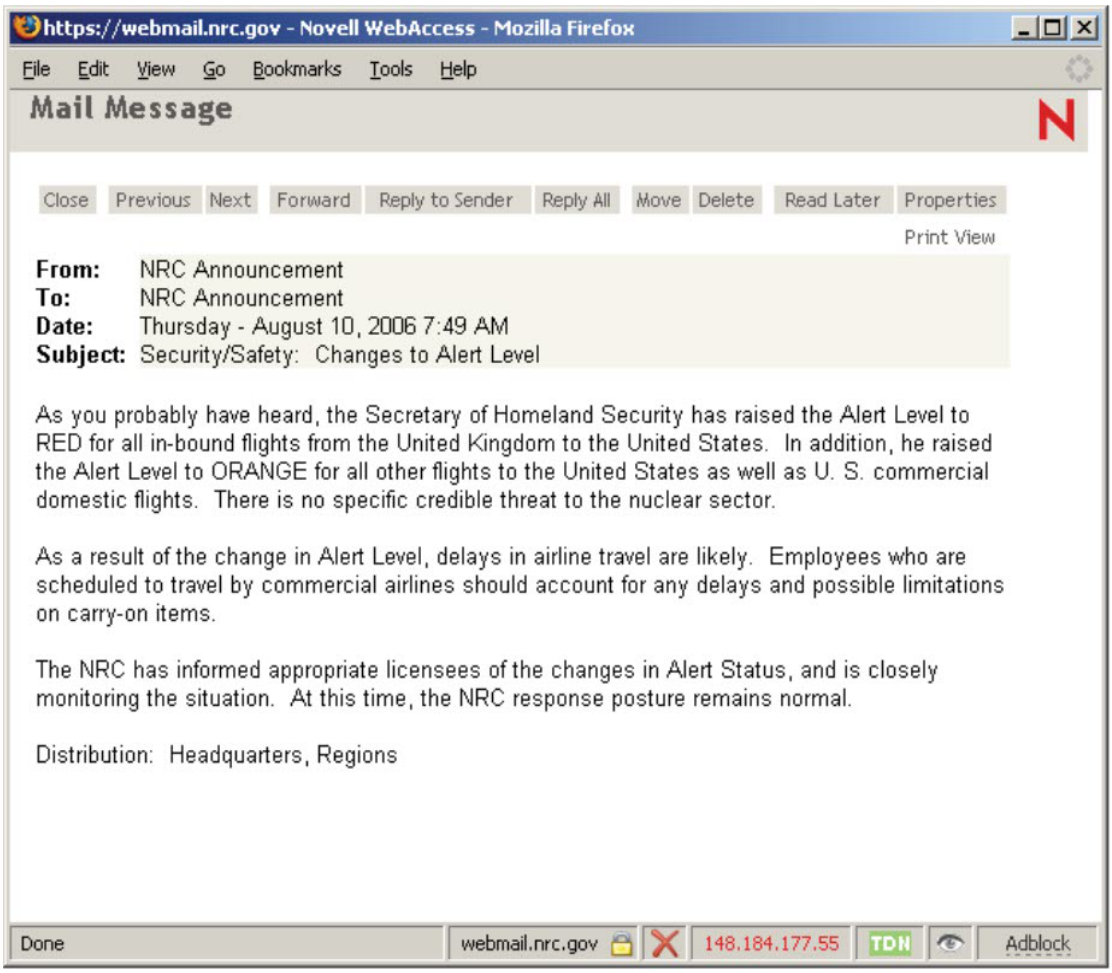


Illustration 8: Sample email The illustration above was pulled from a hacked NRC user account as a sample of email.

Access to E-mail

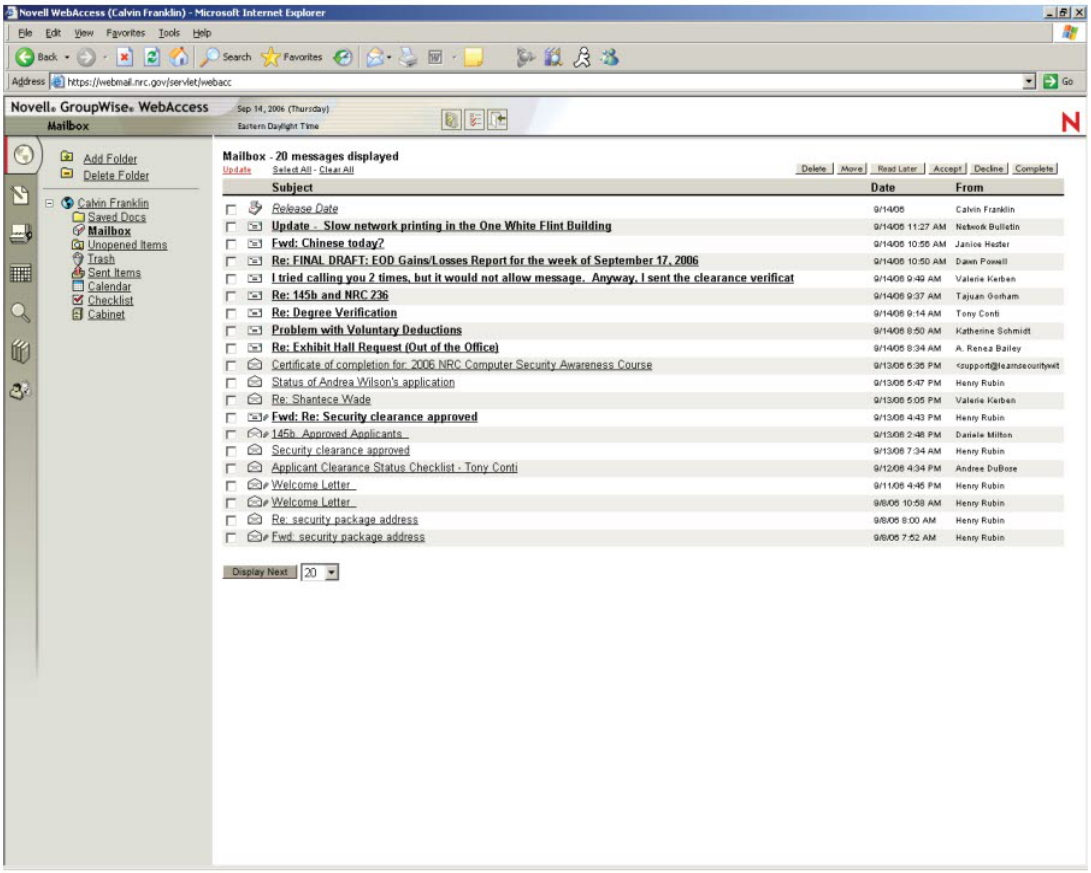


Illustration 9: Second account access The above illustration is a screen capture of a hacked e-mail account. In this case, the SE Team posed as an employee who had forgotten his/her password. The administrator did not request additional authentication outside of the user name and immediately changed the password to a default, thereby allowing the Team access.

SECURITY ALERT: SECURITY AWARENESS TRAINING

Receipt of this email indicates that you have failed to complete the required 2006 Security Awareness Training (SAT). This course must be completed by close of business in order to ensure NRC compliance with the Federal Information Systems Management Act (FISMA) reporting requirements, and are reviewed by Congress and the Office of Management and Budget (OMB) for compliance with other applicable laws.

To complete the 2006 Security Awareness Training, please click on the following link: http://sat.nrc.gov/2006/sat. This training will take approximately 15 minutes and will ensure that the NRC succeeds in protecting its mission critical information and dedication to IT Security.

Thank You for your cooperation.

Illustration 10: Phishing : The above e-mail was generated by the SE Team as a phishing attempt. The link provided would have taken the user to a dead link, although it would have simultaneously gathered specific information about the user and their workstation, which would later be used in a hacking attempt. In this case, the NRC e-mail servers effectively blocked the e-mail and terminated our connection.

Sample Counterfeit Badge

Illustration 11: Badge Information gathering at local restaurants allowed the SE Team to identify specific information about badges. This information allowed the team to duplicate the badge to a high level of detail. Having a badge visible in public whether attached to clothing or some other item, allows others to photograph or obtain enough details about the badge to duplicate the physical appearance. The illustration above is rendering of a NRC contractor badge using a rather simple drawing application. This badge may be used to gain access to facilities then use other techniques such as "piggy backing" to gain access to other sensitive areas.

CONSOLIDATED LIST OF RECOMMENDATIONS

1. Additional information should be required to verify the identity of the user before making changes to system accounts (e.g., the resetting of passwords).

2. A temporary random password should be generated as opposed to using a standard default.

3. NRC should eliminate any open points of connectivity inside the PDR, as it could allow unauthorized users to access the NRC exchange.

4. The NRC Help Desk should be required to identify users, particularly after receiving notification of overt hacking attempts, before making changes to account information.

5. NRC should take steps to ensure that hackers are not able to establish "attack profiles," which generally consist of any information that allows the hacker to establish credibility or pose as an identified target.

6. Access from within the PDR should be restricted only to ADAMS, the NRC's retrievable records system. Internet access should be restricted to only those sites trusted and required to obtain authorized documents.

7. Strict controls should be implemented on PDR systems to prevent malicious users from downloading new viruses, worms, malware, or hacking software from within the PDR.

8. Laptops and other computer equipment taken into the NRC PDR should not be allowed access NRC networks. PDR should place restrictions and other mitigating controls on all internet and network access points.

9. The NRC should enforce existing policy to prohibit employees or visitors from bringing any electronic devices capable of capturing images of the NRC White Flint 1 and 2 facilities.

10. Security should verify visitors' login information and visitors' identity with valid photo identification.

May 21, 2008

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

FROM: Stephen D. Dingbaum **/RA/**
Assistant Inspector General for Audits

SUBJECT: MEMORANDUM REPORT: AUDIT OF NRC'S CONTINUITY OF OPERATIONS PLAN (OIG-08-A-10)

This memorandum reports on the results of our audit of the U.S. Nuclear Regulatory Commission's (NRC) continuity of operations plan (COOP) as related to COOP facilities. NRC does not satisfy Federal or internal agency guidance for security surveys of COOP facilities. Specifically, NRC does not conduct the required annual security surveys of its continuity facilities, and does not systematically document the results of the surveys because the staff appeared unfamiliar with the requirements. As a result, NRC lacks assurance as to the security status of the continuity facilities and may not have information needed to identify and remedy vulnerabilities.

BACKGROUND

Federal Law Requires NRC To Develop and Implement a Continuity of Operations Program

Overall, the NRC's mission is to license and regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety. Should a natural disaster, technological failure, or hostile action threaten NRC's ability to perform or manage this mission from its headquarters facility, agency officials may determine or may be directed that emergency conditions warrant COOP activation. Once the decision has been made to activate COOP, the agency must be prepared to perform essential functions as soon as possible with

minimal disruption of operations, but in all cases within 12 hours of activation and until normal business activities can be reconstituted. The agency's priority mission essential functions – threat assessment, incident response, and emergency communications – must commence in less than 4 hours. The secondary mission essential functions – licensing, inspection, enforcement, and communication with the general public – must commence within 12 hours.

Federal law mandates that Federal agencies develop and implement policies, plans, and readiness measures to mobilize for, respond to, and recover from a national security emergency. Together, these policies, plans, and measures form the basis of an agency's COOP. The Department of Homeland Security has overall responsibility for developing Federal COOP guidelines, and issued Federal Preparedness Circular (FPC) 65[1] as guidance to Federal Executive Branch departments and agencies for contingency plans and programs. The National Security Presidential Directive-51/Homeland Security Presidential Directive-20[2] establishes a comprehensive national policy on the continuity of operations within the Federal Government. This directive also defines minimum communications requirements for Federal agencies' designated COOP facilities.

The Executive Director for Operations approved the agency's COOP in August 2007. This plan was designed as a stand-alone document with 16 annexes. These annexes form the basis of COOP and can be updated and approved by program office directors, as necessary.

The Office of Nuclear Security and Incident Response (NSIR) develops NRC's COOP, and would coordinate agency operations during a COOP event. However, responsibility for managing the agency's COOP infrastructure and assets lies with other NRC organizations. For instance, the Office of Administration's Division of Facilities and Security is responsible for evaluating headquarters, regional continuity facilities, and other regional response centers and ensuring that these facilities meet agency standards for safeguarding NRC personnel and protecting sensitive information.

[1] Federal Preparedness Circular 65, "Federal Executive Branch Continuity of Operations," June 15, 2004. In February 2008, the Department of Homeland Security issued Federal Continuity Directive 1, "Federal Executive Branch National Continuity Program and Requirements," which supersedes FPC 65. Federal Continuity Directive 1 includes facility requirements that are similar to those of FPC 65.

[2] National Security Presidential Directive-51 and Homeland Security Presidential Directive-20, May 9, 2007.

PURPOSE

This audit's initial objective was to determine if NRC's COOP enables the agency to maintain essential functions during an emergency and adhere to Federal continuity of operations criteria and guidelines.[3] However, the objective was subsequently narrowed to assess NRC's compliance with requirements for security surveys of COOP facilities.

FINDING

Federal and NRC Guidance Require Evaluation of COOP Facilities

(b)(7)(F)

NRC Does Not Conduct Required Security Surveys of COOP Facilities

NRC does not conduct required annual surveys of headquarters or its regional continuity facilities, and does not systematically document results of security surveys. Despite Department of Homeland Security and internal agency guidance requiring annual security surveys of facilities that provide the agency with essential COOP capabilities, responsible Division of Facilities and Security staff told OIG auditors that their office aims to conduct security surveys of high-priority sites in 36-month cycles. When asked for documentation of these surveys, agency staff provided reports from a broad range of dates that reflect neither annual nor 36-month survey cycles. In fact, one report for a regional facility captured work performed in 1982. Moreover, only two of these reports specifically mentioned regional Incident Response Centers. Table 1 shows the distribution and date range of security survey reports provided to OIG auditors.

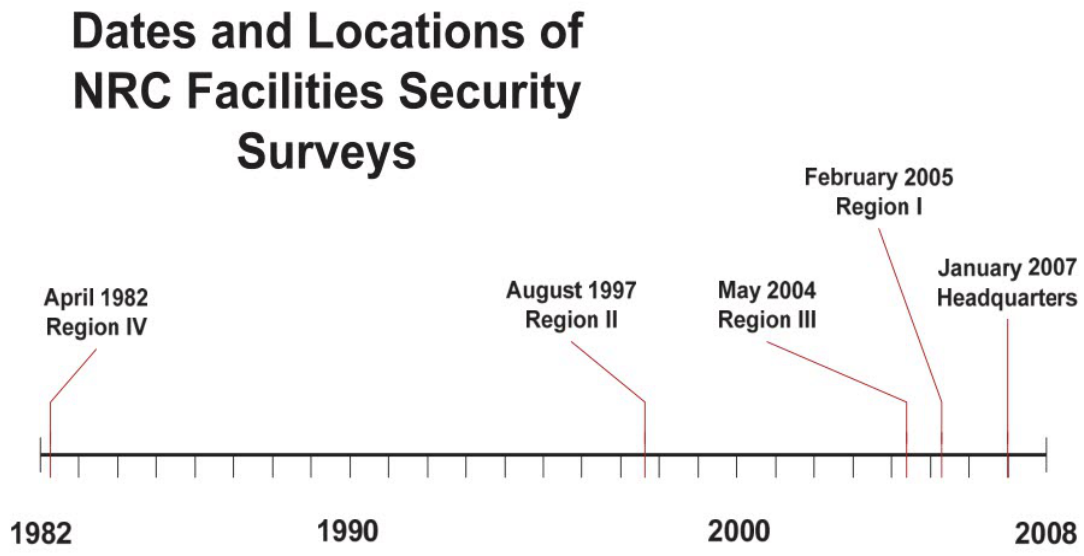


Table 1: Security surveys performed at NRC headquarters and regional facilities, by survey year.

The inconsistency of records on file and the wide date range of security surveys indicate that NRC is not adequately managing documentation needed to provide agency staff with timely information regarding the security status of the continuity facilities.

Key Staff Lack Understanding of Security Evaluation Requirements

NRC does not conduct annual security assessments of its continuity facilities because staff are unfamiliar with both Federal and internal agency requirements. For example, when questioned about the basis for conducting site security surveys in 36-month

cycles rather than annual cycles, Division of Facilities and Security staff told auditors that this was an "office goal." In addition, the agency official responsible for overseeing the security survey program was uncertain whether headquarters, the regional continuity facilities, and the other regional response centers had been properly assessed because he was new to the job. Although NSIR has overall responsibility for NRC's COOP program, agency guidance assigns primary responsibility to the Division of Facilities and Security for ensuring that NRC facilities—including essential continuity sites—meet basic requirements for information and physical security.

NRC Lacks Assurance of the Security Status of the COOP Facilities

Without conducting required annual security surveys of agency continuity facilities and appropriate documentation of survey results, NRC may not be able to identify and correct potential security vulnerabilities and technical shortfalls that could compromise operations.

RECOMMENDATIONS

(b)(7)(E)

AGENCY COMMENTS

(b)(6)

SCOPE AND METHODOLOGY

To accomplish the audit's objective, auditors evaluated NRC's COOP to assess NRC's compliance with requirements for security surveys of COOP facilities.

Auditors interviewed staff at headquarters and offices in NRC Regions I and IV to learn their roles and responsibilities as they pertain to the development, implementation, and management of the COOP and the supporting infrastructure. Also, auditors toured the Mount Weather Emergency Operations Center to observe the benefits this location could provide to the agency's COOP program.

Auditors reviewed applicable Federal directives and reports establishing the policy and procedures for the COOP Program. Those documents included the National Security Presidential Directive-51/Homeland Security Presidential Directive-20, the Federal Preparedness Circular-65, the National Security Communications Directive 3/10, and the United States Public Law 106-346 – Federal Telecommuting Program. NRC documents reviewed included the COOP and its annexes, Management Directive and Handbook 12.1, physical security survey reports, and the Network Continuity of Operations Plan.

This work was conducted from May 2007 through December 2007, in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The work was conducted by Beth Serepca, Team Leader; Shyrl Coker, Audit Manager; and David Ditto, Senior Management Analyst.

Attachment: As stated:

cc: Chairman Klein
Commissioner Jaczko
Commissioner Lyons
Commissioner Svinicki

Electronic Distribution

Frank P. Gillespie, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jim E. Dyer, Chief Financial Officer
Margaret M. Doane, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
Bruce S. Mallett, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Waste, Research, State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director for Information Services and Chief Information Officer, OEDO
Vonna L. Ordaz, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Cynthia A. Carpenter, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials and Environmental Management Programs
Guy P. Caputo, Director, Office of Investigations
Thomas M. Boyce, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Michael R. Johnson, Director, Office of New Reactors
Michael F. Weber, Director, Office of Nuclear Material Safety and Safeguards
Eric J. Leeds, Acting Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
Victor M. McCree, Acting Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Elmo E. Collins, Jr., Regional Administrator, Region IV

Instructions for Responding to OIG Report Recommendations
Instructions for Action Offices

Action offices should provide a written response on each recommendation within 30 days of the date of the transmittal memorandum or letter accompanying the report. The concurrence or clearance of appropriate offices should be shown on the response. After the initial response, responses to subsequent OIG correspondence should be sent on a schedule agreed to with OIG.

Please ensure the response includes:

1. The report number and title, followed by each recommendation. List the recommendations by number, repeating its text verbatim.

2. A management decision for each recommendation indicating agreement or disagreement with the recommended action.

    a. For agreement, include corrective actions taken or planned, and actual or target dates for completion.

    b. For disagreement, include reasons for disagreement, and any alternative proposals for corrective action.

    c. If questioned or unsupported costs are identified, state the amount that is determined to be disallowed and the plan to collect the disallowed funds.

    d. If funds put to better use are identified, then state the amount that can be put to better use (if these amounts differ from OIG's, state the reasons).

OIG Evaluation of Responses

If OIG concurs with a response to a recommendation, it will (1) note that a management decision has been made, (2) identify the recommendation as resolved, and (3) track the action office's implementation measures until final action is accomplished and the recommendation is closed.

If OIG does not concur with the action office's proposed corrective action, or if the action office fails to respond to a recommendation or rejects it, OIG will identify the recommendation as unresolved (no management decision). OIG will attempt to resolve the disagreement at the action office level. However, if OIG determines that an impasse has been reached, it will refer the matter for adjudication to the Chairman.

Semiannual Report to Congress

In accordance with the Inspector General Act of 1978, as amended, OIG is required to report to Congress semiannually on April 1 and October 1 of each year, a summary of each OIG report issued for which no management decision was made during the previous 6-month period. Heads of agencies are required to report to Congress on significant recommendations from previous OIG reports where final action has not been taken for more than one year from the date of management decision, together with an explanation of delays.

EVALUATION REPORT

~~OFFICIAL USE ONLY~~

Social Engineering Assessment Report

OIG-10-A-11 March 16, 2010

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

March 16, 2010

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

FROM: Stephen D. Dingbaum **/RA/**
Assistant Inspector General for Audits

SUBJECT: SOCIAL ENGINEERING ASSESSMENT REPORT
(OIG-10-A-11)

Attached is the Office of the Inspector General's (OIG) *Social Engineering Assessment Report.*

The report presents the results of the subject report. Agency comments provided during and subsequent to a January 26, 2010, exit conference have been incorporated, as appropriate, into this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at 415-5915 or (b)(7)(C)

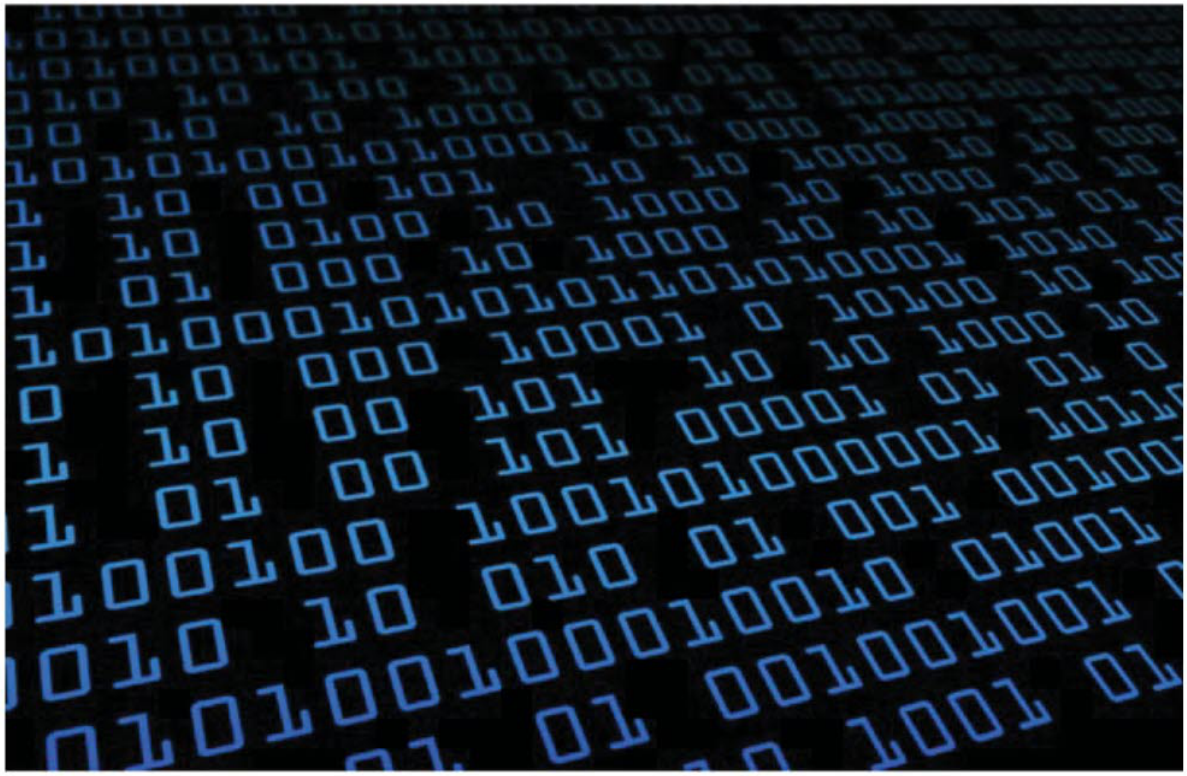
Attachment: As stated

Electronic Distribution

Edwin M. Hackett, Executive Director, Advisory Committee on Reactor Safeguards
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Stephen G. Burns, General Counsel
Brooke D. Poole, Jr., Director, Office of Commission Appellate Adjudication
James E. Dyer, Chief Financial Officer
Margaret M. Doane, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
R. William Borchardt, Executive Director for Operations
Bruce S. Mallett, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Waste, Research, State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director for Corporate Management and Chief Information Officer, OEDO
Nader L. Mamish, Assistant for Operations, OEDO
Kathryn O. Greene, Director, Office of Administration
Patrick D. Howard, Director, Computer Security Officer
Roy P. Zimmerman, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials and Environmental Management Programs
Cheryl A. McCrary, Director, Office of Investigations
Thomas M. Boyce, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Michael R. Johnson, Director, Office of New Reactors
Michael F. Weber, Director, Office of Nuclear Material Safety and Safeguards
Eric J. Leeds, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
James T. Wiggins, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
Luis A. Reyes, Regional Administrator, Region II
Mark A. Satorius, Regional Administrator, Region III
Elmo E. Collins, Jr., Regional Administrator, Region IV

U.S. Nuclear Regulatory Commission
Office of the Inspector General (OIG)

Social Engineering Assessment Report



March 2010

~~OFFICIAL USE ONLY – SECURITY RELATED INFORMATION~~

Table of Contents

1. Executive Summary

Between July 22nd, 2009 and November 9th, 2009, the U.S. Nuclear Regulatory Commission (NRC) Office of Inspector General (OIG), with the support of PricewaterhouseCoopers, LLP (PwC), assessed the effectiveness of Agency security controls designed to mitigate the risk of social engineering attacks. (b)(7)(E) assessment included reconnaissance, dumpster/recycle bin diving and workspace walkthroughs, physical access assessment, baiting, phone calls, and e-mail phishing.

Through these activities, the assessment team demonstrated that the NRC established effective controls in certain areas and addressed weaknesses identified in a prior assessment completed on November 30th, 2006 (OIG-07-A-04). Specifically, the testing team noted the following improvements:

- Employees protected badges when leaving the NRC campus, preventing the assessors from successfully obtaining clear photographs or capturing badge numbers and bar codes.
- Individuals that detected social engineering attacks reported such incidents to the NRC Computer Incident Response Team (CIRT).
- Internal security assessment activities were detected by the Office of Information Systems (OIS) and reported to the appropriate points of contact.
- Controls designed to secure the Public Document Room (PDR) had been enhanced to address previously identified weaknesses, which prevented the assessors from accessing the Internet and the internal NRC local area network (LAN) from PDR workstations.
- PDR personnel were alert and prevented the assessors from connecting laptops or removing network cabling.

However, the assessment also revealed additional areas where NRC can further strengthen the controls necessary to protect against social engineering attacks. Specifically, the following high-level weaknesses were identified:

- NRC employees and contractors were susceptible to social engineering attacks, and provided usernames, passwords, and badge numbers to the assessment team.
- NRC employees and contractors improperly stored and discarded sensitive documents, information, and other materials.
- NRC employees and contractors failed to prevent unauthorized access to controlled locations within the One White Flint North (OWFN) building.
- Technical security controls failed to prevent unauthorized access to internal and external information systems.
- Information that was used to facilitate social engineering attacks was accessible via the NRC public website.

This report includes **12** detailed recommendations designed to help NRC address the identified gaps. These recommendations, listed in Section 5, include enhancing security awareness training, strengthening facility security policies and procedures, implementing and maintaining enhanced technical security controls to mitigate social engineering attacks, and limiting publicly accessible data to reduce the availability of information that may be leveraged to conduct social engineering attacks. At the exit conference for the assessment, NRC management concurred with the findings, and requested that we consolidate some of the recommendations in the draft report. NRC management officials also noted that current security awareness training addresses user responsibilities related to many of the areas covered by the assessment, and that they intend to focus on augmenting the training with other awareness techniques and periodically evaluating its effectiveness.

2. Background

Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. Social engineers will commonly use the telephone or Internet to trick a person into revealing sensitive information or getting them to do something that is against typical policies, exploiting the natural tendency of individuals to trust others. A contemporary example of a social engineering attack is the use of e-mail attachments that contain malicious payloads (that, for instance, use the victim's machine to send massive quantities of spam). After earlier malicious e-mails led software vendors to disable automatic execution of attachments, users now have to explicitly activate attachments for this to occur. Many users, however, will blindly click on any attachments they receive, thus allowing the attack to work.

The NRC OIG had a need for assessing the effectiveness of the security policies and control measures protecting sensitive information technology systems against a social engineering attack. To assist in this effort, the OIG selected PwC to execute an assessment of NRC security controls designed to prevent and respond to social engineering attacks. The results of this assessment are detailed within this report and are organized into the following sections:

- Methodology and approach
- Assessment results and recommendations
- Appendices

Contractor services were performed and this report was developed in accordance with our contract GS-35F-0263P and Task Order Number 040921366 dated 7/22/2009, and are subject to the terms and conditions included therein.

Contractor services were performed in accordance with Standards for Consulting Services established by the American Institute of Certified Public Accountants (AICPA). Accordingly, we are providing no opinion, attestation, or other form of assurance with respect to our work and we did not verify or audit any information provided to us.

Contractor work was limited to the specific procedures and analysis described herein and was based only on the information made available through November 9th, 2009. Accordingly, changes in circumstances after this date could affect the findings outlined in this report.

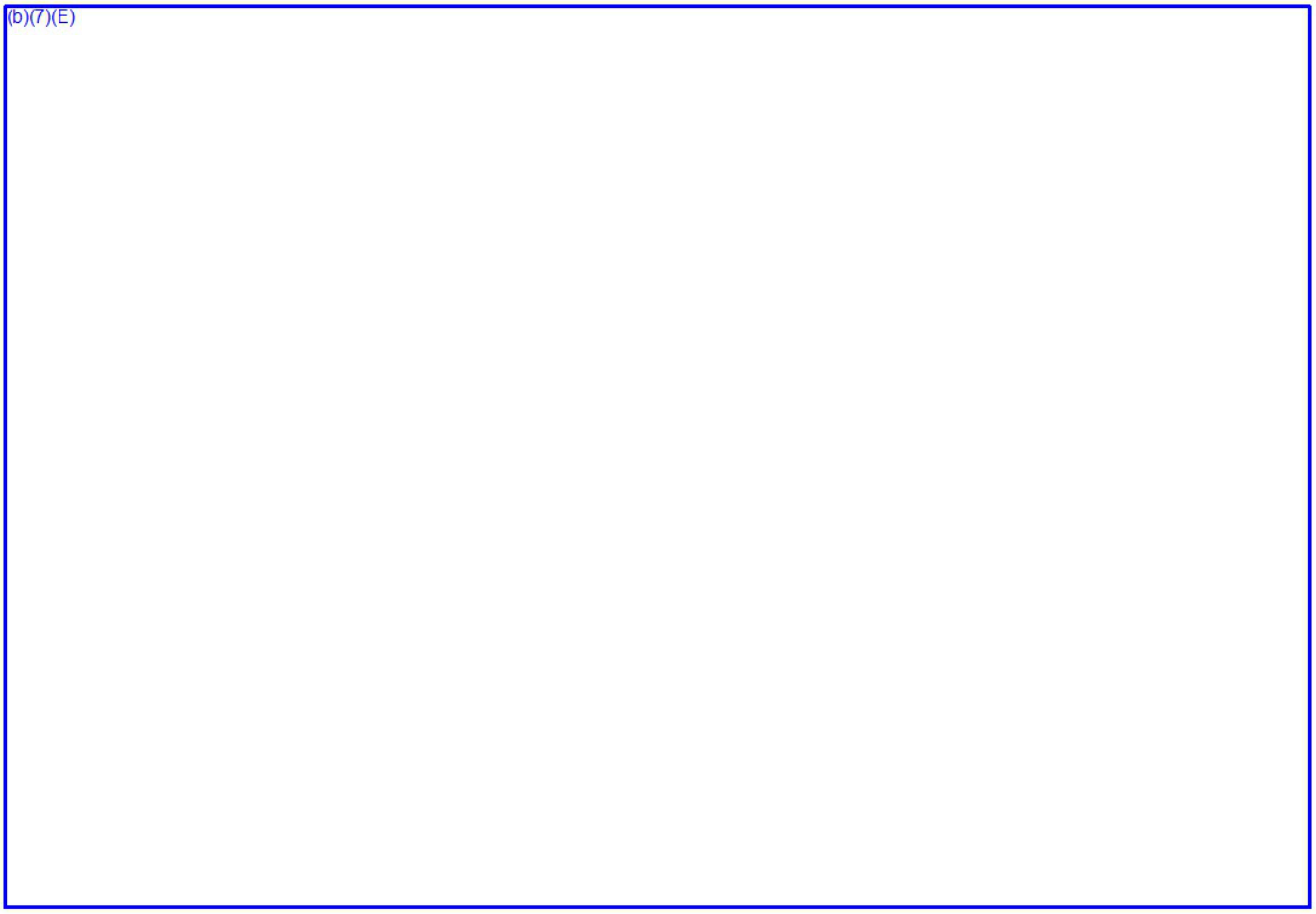
This information has been prepared solely for the use and benefit of, and pursuant to a client relationship exclusively with, the NRC and the U.S. Government. PwC LLC disclaims any contractual or other responsibility to others based on its use and, accordingly, this information may not be relied upon by anyone other than NRC and the U.S. Government. The report may be subject to release under the U.S. Freedom of Information Act ("the Act"). Unless required by the Act, neither the report nor its content may be distributed to, discussed with or otherwise disclosed to any Third Party without the prior written consent of PwC. If the report is requested under the Act, NRC has agreed to promptly notify PwC of such request as required by federal law.

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)



(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

5. Recommendations

The following are the recommendations associated with the findings of the assessment.

Procedural Recommendations

1. Implement secure coding practices within the SDLC and continuously monitor web applications for security vulnerabilities:
    a. Implement appropriate input validation mechanisms and integrate secure coding into the SDLC.
    b. Perform web application security assessments (WASA) as part of the continuous monitoring process.
2. Review logs, identify suspicious events and flag for further investigations, and take actions to limit the impact of events determined to be the result of malicious activity.
3. Assess and continually monitor publicly facing information for sensitive or unnecessary information:
    a. Continuously monitor publicly facing information and remove or limit sensitive information, such as potentially extraneous information included in the NRC Telephone Directory.
    b. Determine if a publicly accessible NRC Telephone Directory is necessary to fulfill the mission of the agency. If not, remove the directory from the external website and ensure it is only visible internally. Alternatively, the NRC can also limit the amount of information provided in the directory, to mitigate the threat of social engineering attacks.

Technical Control Recommendations

4. Restrict systems from accepting anonymous connections and enforce strong authentication controls:
    a. Discontinue the use of externally accessible, anonymous instances of Citrix in favor of a more secure enterprise application.
    b. Disable null (anonymous) sessions on domain controllers and workstations within the NRC, where feasible.
    c. Implement strong passwords and enforce the use of strong passwords for users in accordance with NRC policies and Federal guidance.
    d. Limit use of local accounts and establish a mechanism to maintain and manage unique passwords for local accounts.
    e. Require two factor authentication, such as HSPD-12 compliant badges or valid NRC certificates, on all Internet-facing applications, including Outlook Web Access.
5. Restrict the use of removeable storage media on NRC computers:
    a. Configure workstations to only accept connections from USB drives approved by the NRC.
    b. Improve controls around PDR computers by disabling USB access or enclosing PDR computers in a locked cabinet.
6. Implement controls to restrict NRC network access to authorized systems and restrict NRC computers from connecting to unauthorized systems:
    a. Do not permit externally facing systems within the demilitarized zone (DMZ) to initiate communications with systems on the internal NRC network.

b. Establish mechanisms to validate that only authorized NRC systems may connect to the NRC network.

c. Configure PDR workstations to only access required systems, using specific ports and protocols.

7. Implement system controls to assist in identifying and limiting the impact of phishing e-mails and malicious files:

   a. Configure the e-mail or anti-spam system to mark e-mails received from non-NRC e-mail addresses to allow employees and contractors to more easily identify external and potentially dangerous e-mails.

   b. Implement technical controls including application whitelisting (configuring allowed applications), browser virtualization (launching browsers in an isolated virtual environment), and web proxies to limit the impact of malicious files or links, which users may inadvertently access.

Security Awareness and Training Recommendations

8. Review security awareness training to ensure it adequately educates users on their responsibilities to:

   a. Protect sensitive media, while providing examples of types of sensitive data.

   b. Properly dispose of sensitive information, while identifying the potential impact on the agency or person when media is not adequately secured in accordance with documented policies.

   c. Understand the risks of connecting unauthorized USB drives to NRC workstations.

   d. Recognize phishing attacks that arrive from non-NRC e-mail addresses and appropriately respond to contained links, attached files, and other malicious tactics leveraged by attackers.

   e. Never provide their password to the Help Desk or any other NRC representative.

   f. Understand that phone numbers can be 'spoofed' and provide instructions on how to identify potentially 'spoofed' phone numbers.

   g. Understand their role in preventing 'piggybacking', as well as the risks associated with allowing unauthorized users to access secure NRC locations.

9. Distribute a message from leadership informing NRC employees and contractors of the threat of social engineering and reiterate that under no circumstances will anyone from the NRC ask for their password via phone or e-mail.

10. Assess the effectiveness of security awareness training, security policies and procedures, and technical controls on a periodic basis. Assessments should include proactive measures such as dumpster/recycle bin diving, workspace walkthroughs, phishing, or social engineering phone calls.

Physical Security Recommendations

11. Revise current policy to restrict visitors from leaving the lobby area without an escort.

12. Evaluate the feasibility of implementing security technologies such as access control turnstiles to limit "piggy-backing" into secure NRC locations.

6. Appendices

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

November 6, 2019

MEMORANDUM TO: Margaret M. Doane
Executive Director for Operations

FROM: Dr. Brett M. Baker /RA/
Assistant Inspector General for Audits

SUBJECT: EVALUATION OF NUCLEAR REGULATORY COMMISSION VULNERABILITY ASSESSMENT AND PENETRATION TESTING (OIG-20-A-02)

The Office of the Inspector General (OIG) contracted RMA Associates, LLC to conduct an assessment of NRC's information technology vulnerabilities and perform penetration testing. Attached is OIG's audit report titled *Evaluation of Nuclear Regulatory Commission Vulnerability Assessment and Penetration Testing*. The objective of this evaluation was to assess the NRC's technical configuration and security controls by performing coordinated network and host-based security testing supporting the FISMA assessment. The findings and conclusions presented in this report are the responsibility of RMA. OIG's responsibility is to provide adequate oversight of the contractor's work in accordance with the Council of the Inspectors General on Integrity and Efficiency, Quality Standards for Inspection and Evaluation.

The report presents the results of the subject audit. Following the October 9, 2019, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

OIG identified observations that, if remediated, would strengthen NRC's security posture. Specifically, improvements can be made in four general information systems control areas (b)(7)(E)

Please provide information on actions taken or planned on each of the recommendation(s) within 30 calendar days of the date of this memorandum. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at (301) 415-5915 or (b)(7)(E)

Attachment: As stated

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Evaluation of

NUCLEAR REGULATORY COMMISSION

Vulnerability Assessment and Penetration Testing

October 18, 2019

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

October 18, 2019

Mr. David Lee
Deputy Inspector General
Nuclear Regulatory Commission
11555 Rockville Pike
Rockville, MD 20852

Re: Evaluation Report on Nuclear Regulatory Commission Vulnerability Assessment and Penetration Testing

Dear Mr. Lee:

RMA Associates, LLC (RMA) is pleased to submit the Evaluation Report on Nuclear Regulatory Commission (NRC) Vulnerability Assessment and Penetration Testing (VA/PT). RMA assessed NRC's information security by performing VA/PT in support of NRC's Federal Information Security Modernization Act of 2014 (FISMA) assessment.

In terms of background, although NRC has a robust security program in place, continuous cybersecurity improvement must be a top priority for NRC, and all Federal Government agencies. While technology enables and enhances the ability to share information instantaneously among stakeholders through computers and networks, it also makes networks vulnerable to malicious activity and exploitation by internal and external sources. Insiders with malicious intent, recreational and institutional hackers, and attacks by foreign intelligence organizations are significant threats to NRC's critical systems.

Specifically, the U.S. Department of Homeland Security recognizes these threats:

"During the last several decades, advances in technology have fundamentally changed the world. Substantial growth in Internet access, use of Internet-enabled devices, and the availability of high-speed information technology systems and large datasets have facilitated productivity, efficiencies, and capabilities across all major industries. The proliferation of technology also presents new cybersecurity challenges and leads to significant national risks. More than 20 billion devices are expected to be connected to the Internet by 2020. The risks introduced by the growing number and variety of such devices are substantial.… Like every organization, no matter how big or small, we must minimize our organizational vulnerability to malicious cyber activity by protecting our own networks.[1]"

We based our assessment and penetration methodology on the signed Rules of Engagement (ROE), which established RMA procedures for conducting electronic security tests for the NRC. The ROE

[1] U.S. Department of Homeland Security, Cybersecurity Strategy May 15, 2018

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

was based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment*.

The ROE documents the scope, objective, and methodology of the network security tests, the procedures to be performed, the rules to be followed, and points of contact. The ROE also provides NRC OIG's and NRC Management's authorization for RMA to conduct these tests. These specific rules were necessary to ensure we performed the testing in a manner that minimized operational impact while maximizing the usefulness value of the test.

We conducted the evaluation in accordance with the Council of Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation.

Sincerely,

Reza Mahbod

Reza Mahbod, CPA, CISA, CGFM, CICA, CGMA, CDFM
President
RMA Associates, LLC

Enclosure

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Table of Contents

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

I. EXECUTIVE SUMMARY

RMA Associates, LLC (RMA) conducted a Vulnerability Assessment and Penetration Testing (VA/PT) of the Nuclear Regulatory Commission (NRC)'s information security in support of NRC's Federal Information Security Modernization Act of 2014 (FISMA) assessment. The testing was based on the approved Rules of Engagement (ROE) between NRC, NRC Office of Inspector General (OIG), and RMA that required the use of National Institute of Standards and Technology (NIST) guidance.

We performed an assessment of NRC's network infrastructure, servers, workstations, applications, and routers in support of NRC's system that can be accessed internally from NRC's networks and accessed externally from the public Internet.

(b)(7)(E)

During our VA/PT, we identified observations that, if remediated, would help strengthen NRC's security posture. In summary, we have categorized our comments within this report into four general information systems control observations:

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

To address these observations, we recommend NRC perform the following:

1. Address security deficiencies identified during the assessments of NRC's applications and network infrastructure, in accordance with CSO-STD-0020, *Organization-Defined Values for System Security and Privacy Controls*.
2. For the vulnerabilities listed in this report, develop a plan and schedule for evaluating the vulnerabilities identified; determine the appropriate action to address the vulnerability (e.g., mitigation, deviation, risk acceptance); and implement the remedial actions.

II. OBJECTIVE

RMA was contracted by the NRC OIG to assess the NRC's technical configuration and security controls by performing coordinated network and host-based security testing supporting the FISMA assessment. Internal controls related to the evaluation objective were reviewed and analyzed. Throughout the evaluation, we considered the possibility of fraud, waste, and abuse in the program.

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

E. Recommendations

To address the vulnerabilities mentioned above, we recommend NRC perform the following:

1. Address security deficiencies identified during the assessments of NRC's applications and network infrastructure, in accordance with CSO-STD-0020, *Organization-Defined Values for System Security and Privacy Controls*.
2. For the vulnerabilities listed in this report, develop a plan and schedule for evaluating the vulnerabilities identified; determine the appropriate action to address the vulnerability (e.g., mitigation, deviation, risk acceptance); and implement the remedial actions.

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

(b)(7)(E)

NRC Webhosting Information

```
OrgName:    Beyond The Network America, Inc.
OrgID:      BNA-42
Address:    520 Herndon Parkway
Address:    Suite E
City:       Herndon
StateProv:  VA
PostalCode: 20170
Country:    US

NetRange:   209.8.0.0 - 209.9.255.255
CIDR:       209.8.0.0/15
NetName:    BTN-CIDR4
NetHandle:  NET-209-8-0-0-1
Parent:     NET-209-0-0-0-0
NetType:    Direct Allocation
NameServer: NS.CAIS.COM
NameServer: NS2.CAIS.COM
Comment:    * Rwhois information on assignments from this block available at:
Comment:    * rwhois.cais.net 4321
RegDate:    1996-12-18
Updated:    2004-11-12

OrgNOCHandle: NOC1582-ARIN
OrgNOCName:   NOC
OrgNOCPhone:  +1-703-621-1637
OrgNOCEmail:  supportamericas@btnaccess.com

OrgTechHandle: JKI101-ARIN
OrgTechName:   Kim, Joon
OrgTechPhone:  +1-703-621-3974
OrgTechEmail:  jkim@pacwglobal.com

# ARIN WHOIS database, last updated 2006-07-17 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Illustration 2: NRC Web information: The illustration above is the "whois" information provided by ARIN on network space for a hosting service used by the NRC. The SE Team used this information to understand NRC partners and additional cyber resources.

NRC Network Space

```
OrgName:    United States Nuclear Regulatory Commission
OrgID:      USNRC
Address:    11545 Rockville Pike
Address:    OCIO/ITID
Address:    Mail Stop T-6 F15
Address:    OCIO/ITID
Address:    Mail Stop T-6 F15
City:       Rockville
StateProv:  MD
PostalCode: 20852
Country:    US

NetRange:   148.184.0.0 - 148.184.255.255
CIDR:       148.184.0.0/16
NetName:    USNRC
NetHandle:  NET-148-184-0-0-1
Parent:     NET-148-0-0-0-0
NetType:    Direct Assignment
NameServer: IGATE.NRC.GOV
NameServer: DNSAUTH1.SYS.GTEI.NET
NameServer: DNSAUTH2.SYS.GTEI.NET
NameServer: NS1.ZONEEDIT.COM
NameServer: NS3.ZONEEDIT.COM
Comment:
RegDate:    1991-01-01
Updated:    2002-06-26

RTechHandle: SDW2-ARIN
RTechName:   Wood, Stanley D.
RTechPhone:  +1-301-415-7211
RTechEmail:  SDW@nrc.gov

OrgTechHandle: SDW2-ARIN
OrgTechName:   Wood, Stanley D.
OrgTechPhone:  +1-301-415-7211
OrgTechEmail:  SDW@nrc.gov

# ARIN WHOIS database, last updated 2006-07-17 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Illustration 3: NRC network lookup This illustration is the "whois" information provided by ARIN on the NRC network space. The SE Team used this information to conduct network reconnaissance and identify potential targets.