Original Due Date: 03/19/2004

Ticket Number: 020040017
Document Date: 02/02/2004
NRR Received Date: 02/04/2004

From:
Charlotte Turner

TACs:
MC1919

To:
J. E. Dyer

*** YELLOW ***

For Signature of:

Routing:
Dyer
Borchardt
Sheron
Craig
Case
NRR Mailroom

Description:
Security Plans for All Personal Computers and Laptops Being Used for Classified and Safeguards Information Processing

Assigned To:
PIMB

Contact:
SUH, GENE Y

Special Instructions:

MEMORANDUM TO THOSE ON THE ATTACHED LIST DATED:

SUBJECT: SECURITY PLANS FOR ALL PERSONAL COMPUTERS AND LAPTOPS BEING USED FOR CLASSIFIED AND SAFEGUARDS INFORMATION PROCESSING

	Mail Stop	
T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste	T-2	E26
G. Paul Bollwerk, III, Chief Administrative Judge, Atomic Safety and Licensing Board Panel	T-3	F23
Karen D. Cyr, General Counsel	O-15	D21
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication	O-16	C1
Jesse L. Funches, Chief Financial Officer	O-17	F3
Hubert T. Bell, Inspector General	T-5	D28
Janice Dunn Lee, Director, Office of International Programs	O-4	E21
Dennis K. Rathbun, Director, Office of Congressional Affairs	O-16	C1
William M. Beecher, Director, Office of Public Affairs	O-2	A13
Annette Vietti-Cook, Secretary of the Commission	O-16	C1
William D. Travers, Executive Director for Operations	O-16	E15
Patricia G. Norry, Deputy Executive Director for Management Services, OEDO	O-16	E15
William F. Kane, Deputy Executive Director for Homeland Protection and Preparedness, OEDO	O-16	E15
Carl J. Paperiello, Deputy Executive Director for Materials, Research and State Programs, OEDO	O-16	E15
Samuel J. Collins, Deputy Executive Director for Reactor Programs, OEDO	O-16	E15
William M. Dean, Assistant for Operations, OEDO	O-16	E15
Ellis W. Merschoff, Chief Information Officer	T-6	F15
Michael L. Springer, Director, Office of Administration	T-7	D57
Frank J. Congel, Director, Office of Enforcement	O-14	E1
Guy P. Caputo, Director, Office of Investigations	O-3	F1
Paul E. Bird, Director, Office of Human Resources	T-3	A2
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights	T-2	F18
Martin J. Virgilio, Director, Office of Nuclear Material Safety and Safeguards	T-8	A23
Jim Dyer, Director, Office of Nuclear Reactor Regulation	O-5	E7
Ashok C. Thadani, Director, Office of Nuclear Regulatory Research	T-10	F12
Paul H. Lohaus, Director, Office of State and Tribal Programs	O-3	C10
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response	T-4	D22a
Hubert J. Miller, Regional Administrator, Region I	RGN-I	
Luis A. Reyes, Regional Administrator, Region II	RGN-II	
James L. Caldwell, Regional Administrator, Region III	RGN-III	
Bruce S. Mallett, Regional Administrator, Region IV	RGN-IV	

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

February 2, 2004

MEMORANDUM TO: Those on the Attached List

FROM: Charlotte L. Turner
Acting Senior Information Technology Security Officer (SITSO)
Office of the Chief Information Officer

Charlotte L. Turner

SUBJECT: SECURITY PLANS FOR ALL PERSONAL COMPUTERS AND LAPTOPS BEING USED FOR CLASSIFIED AND SAFEGUARDS INFORMATION PROCESSING

Management Directive (MD) 12.5, *NRC Automated Information Security Handbook*, implements the requirements of the Federal Information Security Management Act (FISMA), which requires that the agency provide automated information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, or destruction. MD 12.5 also specifies that Office Directors and Regional Administrators must ensure that information systems sponsored by their office that process or store classified information, Safeguards Information (SGI), or sensitive information have individual security plans.

A template that can be used to develop a security plan for any personal computer or laptop that is used for classified and/or SGI processing is attached and can be accessed through ADAMS using Accession Number ML040220713. Boilerplate is included in the template and any information contained within <> should be replaced with the appropriate information for the personal computer or laptop that is being used for classified and/or safeguards information processing. Instructions for filling in the template are also attached and can be accessed through ADAMS using Accession Number ML040220734. Both files are contained in a package and can be accessed together through ADAMS using Accession Number ML040220684.

The due date for maintaining a centralized file containing this information is April 1, 2004. Please provide an appropriate security plan for each personal computer or laptop that is used or will be used for classified and/or SGI processing by March 19, 2004, to Mrs. Kathy Lyons-Burke. She can be reached at (301) 415-6595 or at kxl3@nrc.gov.

Attachments: As stated

Nuclear Regulatory Commission Security Plan Instructions for Stand-alone Personal Computers and Laptops used for Classified and Safeguards Information Processing

January 16, 2004

Table of Contents

1 SYSTEM DESCRIPTION

Provide the name, location, phone number with area code, and email address for the system owner. Provide the same information for the individual with technical knowledge of the system. State whether or not the system is in active use. If multiple systems have the same purpose, users, and location, you can use a single plan for all of those systems.

1.1 Location

Describe the location of the ADP system during use and when not in use.

1.2 Information

Indicate the level of protective concern associated with the data on the ADP system. This indication is required with regards to the confidentiality, integrity, and availability of the data on the system. For each of the confidentiality, integrity, and availability categories, indicate whether the impact is low, medium, or high if the information is compromised. Listed below are excerpts from *Federal Information Processing Standard 199 - Standards for Security Categorization of Federal Information and Information Systems* and from Management Directive (MD) 12.5, *NRC Automated Information Security Program* to assist in making these determinations.

CONFIDENTIALITY	FIPS 199	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information..." [44 U.S.C., Sec. 3542] A loss of *confidentiality* is the unauthorized disclosure of information.
	NRC MD 12.5	The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.
INTEGRITY	FIPS 199	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity..." [44 U.S.C., Sec. 3542] A loss of *integrity* is the unauthorized modification or destruction of information.
	NRC MD 12.5	Sound, unimpaired, or perfect condition. The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data have when they have not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
AVAILABILITY	FIPS 199	"Ensuring timely and reliable access to and use of information..." [44 U.S.C., Sec. 3542] A loss of *availability* is the disruption of access to or use of information or an information system.

NRC MD 12.5 A state in which AIS resources are in the place needed by the user at the time the user needs them, and in the form needed by the user.

LOW FIPS 199 The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
(ii) result in minor damage to organizational assets;
(iii) result in minor financial loss; or
(iv) result in minor harm to individuals.

MODERATE FIPS 199 The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
(ii) result in significant damage to organizational assets;
(iii) result in significant financial loss; or
(iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

HIGH FIPS 199 The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
(ii) result in major damage to organizational assets;
(iii) result in major financial loss; or
(iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

1.3 Components

1.3.1 Hardware

Describe all ADP hardware that is directly connected to the ADP system (e.g. printers, monitors), including property numbers.

1.3.2 Software

Describe all software (e.g. Windows NT, WordPerfect) installed on the ADP system, including version information. Include any information about encryption used to protect the information on the system.

1.4 Period of Operation

Describe the intended operating hours and days (e.g. normal business hours) of the ADP system.

1.5 Data Integrity and Maintenance of Permanent Records

Describe the mechanisms used to ensure the integrity of the data stored on the system and the method used to maintain a permanent record of the data.

2 INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

A system owner designates the ISSO of a system using a written designation letter or memorandum. The ISSO is responsible for ensuring compliance with NRC's IT security policies and procedures. A full list of ISSO responsibilities can be found in MD 12.5, Section 2.4 Information System Security Officer (ISSO). This plan must be updated any time the ISSO or Alternate ISSO changes.

2.1 Primary ISSO

Provide the ISSO's name, office/organization name, office location, phone number, and email address.

2.2 Alternate ISSO(s)

Provide the alternate ISSO's name, office/organization name, office location, phone number, and email address.

3 NATURE OF ADP ACTIVITY

3.1 Classification Levels

Indicate all the classification levels (e.g. unclassified, SGI, Secret, Top Secret, SCI) to be processed on this system. Indicate for each classification level the percentage of time the computer use is dedicated for processing at that level.

3.2 Types of ADP Activity

Describe the types of ADP activity (e.g. word processing, spreadsheets, graphics, simulations) that will be performed on the system.

4 AUTHORIZED ACCESS

4.1 Users

Either list the authorized users' names, office names, office locations, phone numbers, and email addresses, or provide the other specific definitive information to determine who has access. Describe the procedure for authorizing a new user and for removing a user from the authorized list. Indicate the approving authority to authorize and remove authorization from a user.

4.2 Mechanism

Describe the system authorization mechanism (e.g. username/password, physical access log) for access to the ADP system.

4.3 Auditing

Describe the activity auditing mechanism for the ADP system. Specifically, describe the operating system auditing controls that are implemented and the information that is recorded for each type of activity (e.g. file creation, file deletion, file modification.) Audit reviews by the ISSO are required at least monthly.

5 CONTROLS

5.1 Physical Access Controls

Describe the physical access controls in place to protect the ADP system from unauthorized access. Indicate the procedures for logging all access to the system.

Describe any considerations relevant to physically protecting the ADP system from unauthorized access (e.g. locking storage, safe.)

5.2 Visitor Controls

Describe the controls in place to ensure visitors do not have any access to the ADP system.

6 HANDLING OF DATA

Describe how each type of data stored in or resulting from the ADP system are handled and protected.

7 OPERATING PROCEDURES

Describe the ADP system operating procedures.

8 REPAIR AND MAINTENANCE

Describe the processes and procedures used for the maintenance of the ADP system.

9 SECURITY COMPROMISES OR FAILURES

Describe the procedure in the event of a compromise or failure.

10 RULES OF BEHAVIOR

Describe the rules of behavior for the ADP system. Please reference MD 12.5, section 2.5 Rules of Behavior for NRC AIS Users, for basic rules of behavior (no need to repeat them in this section.) This section of this plan should clearly delineate additional responsibilities and expected behavior of all individuals with access to this system. Specifically include the rules/processes for properly handling classified and SGI information. The rules should state the consequences of inconsistent behavior or noncompliance. The rules should be in writing, and all users must sign indicating that they are aware of the rules of behavior before being granted access to the system. These rules should be developed on a separate sheet of paper. The ISSO shall maintain copies of the sheets signed by each user.

Nuclear Regulatory Commission
Security Plan Template for
Stand-alone Personal Computers and Laptops
used for
Classified and Safeguards Information (SGI) Processing

January 16, 2004

Automated Data Processing (ADP) Security Plan for

<Desktop Personal Computer, Laptop> NRC # <tag number(s)>

NRC Office/Organization Name

Revision #

Date

Table of Contents

1 SYSTEM DESCRIPTION

<Desktop Personal Computer, Laptop> NRC # <tag number(s)> is owned by <name of owner>. <Name of owner> can be located at <region>, <building and room number>, <phone number including area code>, and <email address>. The individual with technical responsibility for the system is <name of technical POC>. <Name of technical POC>> can be located at <region>, <building and room number>, <phone number including area code>, and <email address>. The system <is/is not> in active use.

1.1 Location

The system is physically stored at <region>, <building name>, <floor>, <room designator> in <locked location information>. The system is physically used at <region>, <building name>, <floor>, <room designator> in <locked location information>.

1.2 Information

The system is considered to be <Mission Critical, listed, other (specify)>.

The confidentiality of the data on the ADP system is to be treated with a <low, moderate, high> level of protection. If the confidentiality of the data is compromised, there would be a **<limited, serious, severe or catastrophic>** adverse effect on organizational operations, organizational assets, or individuals.

The integrity of the data on the ADP system is to be treated with a <low, moderate, high> level of protection. If the integrity of the data is compromised, there would be a **<limited, serious, severe or catastrophic>** adverse effect on organizational operations, organizational assets, or individuals.

The availability of the data on the ADP system is to be treated with a <low, moderate, high> level of protection. If the availability of the data is compromised, there would be a **<limited, serious, severe or catastrophic>** adverse effect on organizational operations, organizational assets, or individuals.

1.3 Components

1.3.1 Hardware

The system is a <Desktop PC, Laptop> with a <removable, resident> hard drive unit. In the secure mode, the <Desktop PC, Laptop> will have the removable hard drive installed. At all other times, the <hard drive, Laptop, Desktop PC> will be removed and will be stored in <the locking container and its location>.

The system consists of the following hardware:

- <Personal computer, Laptop>: <Brand> <Model> - NRC # <tag number>
- Monitor: <Brand> <Model> - NRC # <tag number>
- RAM: <amount of RAM>

- Hard drive: <size> removable hard drive
- <number> 3.5 inch floppy drive(s)
- <number> Read/write CD-ROM drive
- <number> Read only CD-ROM drive
- <number> Read only DVD drive
- <number> Read/write DVD drive
- list any other drives
- Scanner: <Brand> <Model>
- Printer: <Brand> <Model>
- Network card: <Brand> <Model>
- Any other hardware that is ever attached to this system during processing

The system <does, does not> have a modem. *(If yes, describe the disabling mechanism)*

The system <does, does not> have LAN connectivity. *(If yes, specify exactly what LAN activity is permitted)*

1.3.2 Software

The system has the following software installed on the drive performing <SGI, classified> processing:

- Operating system: <OS name>, <version>, <service packs installed>
- Antivirus software: <software name>, <version>, <frequency of updates to signatures>, <method of signature update>
- Encryption software: <software name>, <version>
- Other software: <software name>, <version>

The display background has been modified to indicate that <SGI, Confidential, Secret, Top Secret, SCI> information is being processed.

1.4 Period of Operation

The system will be used <during regular business hours, off hours>, <Monday through Friday from 7:30 AM to 4:15 PM>.

1.5 Data Integrity and Maintenance of Permanent Records

The integrity of data on the system is ensured by <implementation of audit, implementation of backup to CD-Rs, rigid version control, etc.> every <number of days, weeks, months>. The integrity of data tasks are performed by the ISSO or alternate ISSO. Permanent records of the information are ensured through <backup to CD-Rs or tape or memory stick, file copy to records management system (like ADAMS), etc.> every <number of days, weeks, months>. Permanent records are generated by the ISSO or alternate ISSO.

2 INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

2.1 Primary ISSO

The primary ISSO for the system is <name of ISSO>. <Name of ISSO> can be located at <region>, <building and room number>, <phone number including area code>, and <email address>.

2.2 Alternate ISSO(s)

The alternate ISSO for the system is <name of ISSO>. <Name of ISSO> can be located at <region>, <building and room number>, <phone number including area code>, and <email address>.

3 NATURE OF ADP ACTIVITY

3.1 Classification Levels

The system will process <unclassified, SGI, Secret, Top Secret, SCI> information. <Percentage> of the system use is devoted to <unclassified, SGI, Secret, Top Secret, SCI> processing.

(If the system will process classified data – provide a reference to the approval received from NSA for the system to process classified data)

3.2 Types of ADP Activity

Activities performed on the system will include <word processing, spreadsheets, graphics, simulations, etc.>.

4 AUTHORIZED ACCESS

All users authorized to access this system have the need to know <and required security clearance>. Prior to being granted system access, each user is required to read this security plan and sign a statement acknowledging their understanding of the requirements and procedures.

4.1 Users

The following personnel are authorized users of this system:

- <authorized user's name>, <office/organization name>, <region>, <office location>, <phone number including area code>, <email addresses>

The list of authorized users is reviewed on a monthly basis to ensure a continued need-to-know. In addition, the list is updated upon user reassignment or termination. New users are added to the list after need-to-know and clearance verification and acknowledgement signature indicating complete understanding of this plan.

<Name of individual authorizing user access> authorizes user access to this system and also removes authorization when appropriate. He/she can be located at <office/organization name>, <region>, <office location>, <phone number including area code>, and <email address>.

4.2 Mechanism

Each system user is assigned a unique username and password to access the system. A password protected screen saver will activate after two minutes of inactivity.

4.3 Auditing

Each user's actions on the system are audited and the audit logs are reviewed at least monthly by the system administrator to identify any inappropriate activity. All auditing is performed by the ISSO or alternate ISSO.

5 CONTROLS

5.1 Physical Access Controls

Physical security is controlled at all entrances to the building by security guards. Each employee is required to present an NRC ID to a security guard. <Describe all physical security considerations that must be taken into account given the location of use. If the system is used at another location, describe the physical security supplied>.

The system is physically protected during use. Physical access to the system during use is limited. Each user records their name and time of access into an access log for the system. <Describe mechanism that limits physical access during use>.

The system is also physically protected when not in use. <Describe mechanism that limits physical access during storage>.

5.2 Visitor Controls

NRC visitors are required to provide picture identification and must be escorted when in the facility. Visitor escorts ensure the visitors do not enter areas where sensitive information is being processed unless they have a purpose approved by the ISSO.

Individuals without a need-to-know are prevented from physical access to the system by <mechanism>.

6 HANDLING OF DATA

The removable hard drive, magnetic media (floppy disks), optical media (CD-ROMs, DVD-ROMs), and all printouts from the system that contain SGI or classified information are properly marked, labeled, and handled according to the applicable procedures in NRC Management Directive (MD) 12.2, "NRC Classified Information Security Program," MD 12.5, "Automated Information Systems Security Program" and MD 12.6, "NRC Sensitive Unclassified Information Security Program," and other applicable procedures provided by the NRC Security Office (ADM), the IT Security Office (OCIO), and the NSIR INFOSEC Office. A copy of the procedures is available to all authorized users.

When not in use, the removable hard drive, all magnetic and optical media, and all printouts or other materials containing <Safeguards, Classified> Information are marked, labeled, stored, protected, and destroyed in accordance with applicable procedures in NRC Management Directive 12.1, "NRC Facility Security Program" and NRC Management Directive 12.2.

7 OPERATING PROCEDURES

The system operating procedures for processing SGI are as follows:

1. Prior to processing
   a. Ensure that only properly cleared personnel with an approved need-to-know are present.
   b. Ensure the monitor screen is positioned away from the entrance to the Safeguards processing area.
   c. Ensure that access to the Safeguards processing area is controlled.
   d. Remove all unclassified magnetic or optical media from the appropriate drives.
2. Processing:
   a. Install required hard drive.
   b. Log into the computer.
   c. Turn on the printer.
   d. If needed, install any necessary magnetic or optical media in diskette or CD-ROM drives. Ensure the media are labeled as Safeguards Information, as appropriate.
   e. Ensure that the background on the screen indicates <Safeguards, Confidential, Secret, Top Secret, SCI> processing.
   f. Begin processing.
3. Processing termination:
   a. Ensure all magnetic or optical media containing safeguards information have been properly marked.
   b. Terminate all safeguards data processing and exit all programs.
   c. Remove all safeguards magnetic and optical media from appropriate drives.
   d. If used, run 3 blank pages through printer and/or scanner or power off the printer and/or scanner.
   e. Shut-down the printer.
   f. Log out of the notebook computer and ensure that the log on screen is present.
   g. Ensure all safeguards materials are accounted for.
   h. Ensure that the notebook computer and all other magnetic and optical media containing Safeguards Information are stored only in appropriate lock-bar file cabinets, or other approved container.
   i. Lock and verify the storage container is closed and locked and log access to the container as necessary.

8 REPAIR AND MAINTENANCE

Contractor maintenance and regional IT support staff personnel may require access to the system for repair and maintenance purposes. When repair or maintenance is required, at least one authorized and knowledgeable NRC employee will be present at all times to monitor the work performed. Should repair or maintenance be required for the notebook computer hard drive or other magnetic or optical media containing safeguards data, only properly cleared repair personnel will be authorized to perform such work and at least one authorized and knowledgeable NRC employee will be present at all times to monitor the work performed. All other classified and safeguards materials will be properly secured in approved containers.

9 SECURITY COMPROMISES OR FAILURES

All security compromises or failures will be reported to the ISSO, the Alternate ISSO, the regional ISSO, the NRC Senior Information Technology Security Officer (SITSO), and the Division of Facilities and Security (ADM/DFS) in accordance with NRC Management Directives 12.1 and 12.2.

10 RULES OF BEHAVIOR

All system users must observe the rules of behavior specified in MD 12.5, section 2.5 Rules of Behavior for NRC AIS Users. In addition, all users must follow the operating procedures outlined in Section 7 of this document. <Clearly delineate additional responsibilities and expected behavior of all individuals with access to this system. Specifically include the rules/processes for properly handling classified and SGI information. The rules should state the consequences of inconsistent behavior or noncompliance.>

11 ACKNOWLEDGMENT STATEMENT

By my signature below, I acknowledge that I have read this Security Plan for <Desktop PC, Laptop> computer # <tag number(s)> and understand the operating procedures and rules of behavior concerning the processing of safeguards information on this system, as well as, my personal responsibilities regarding the protection and storage of all <SGI, classified> materials to include the notebook computer, magnetic and optical media, and all printouts containing <SGI, classified> material or other <SGI, classified> materials.

PRINT Name Signature Date