POLICY ISSUE

INFORMATION

May 21, 2009 SECY-09-0077

FOR: The Commissioners

FROM: R. W. Borchardt
Executive Director for Operations

SUBJECT: INFORMATION SECURITY STRATEGIC PLAN

PURPOSE:

The purpose of this paper is to inform the Commission of the U.S. Nuclear Regulatory Commission (NRC) staff's development of the enclosed draft Information Security Strategic Plan (ISSP) and the intent to distribute the document for comment to external stakeholders.

BACKGROUND:

On November 14, 2007, the Commission directed the staff to develop a comprehensive information security (IS) strategy in Staff Requirements Memorandum (SRM) S07-0181, "Proposed Establishment of the Computer Security Office." IS relates to the protection of data in all forms (including both electronic and physical) from unauthorized access, use, disclosure, destruction, modification, or disruption. Most offices within the NRC have some level of IS responsibility, either from an internal agency perspective or from an external (i.e., regulatory) perspective, or both.

In response to the November 2007 SRM, and at the direction of the Deputy Executive Director for Corporate Management (DEDCM), in January 2008 an NRC staff working group sponsored by the Computer Security Office (CSO) began developing the ISSP, including how the strategies in the ISSP interface with strategies in other NRC offices.

CONTACT: Kathy L. Lyons-Burke, CSO/PSTT
301-415-6595

Scott A. Morris, NSIR/DSP, 301-415-7083

During the early stages of the CSO working group activities, several questions involving potential cyber security controls at nuclear power plants were raised. In the past, these types of questions or issues would be addressed in a somewhat “ad hoc” fashion, in part because of the small number and dispersed staff within the agency who possessed the necessary information technology security (i.e., cyber security) expertise. Recognizing the need to address these issues in a more planned and consistent manner, in May 2008 senior agency management established the Information Security Steering Committee (ISSC) (Agencywide Documents Access and Management System (ADAMS) Accession No. ML081080511) to oversee the development of the agencywide ISSP. In addition, the ISSC initiated the establishment of a formal agency process to efficiently and effectively assess and assist the agency in resolving emergent cyber security-related issues and incidents affecting nuclear facilities.

The ISSC is comprised of senior managers from NRC program offices that have IS oversight responsibilities. The DEDCM and the Deputy Executive Director for Reactor and Emergency Preparedness Programs co-chair the steering committee. The committee charter established working groups for the preparation of the ISSP and response to emergent cyber security issues (ADAMS Accession No. ML082750461). This paper focuses on the ISSP. The staff provided a separate memorandum (ADAMS Accession No. ML090070209) on April 9, 2009, to address ISSC development of the Cyber Issue Assessment Process and the establishment of a Cyber Assessment Team.

DISCUSSION:

Over the past year, members of the ISSP working group met frequently to discuss the existing agency IS activities, as well as any recognized areas for improvement, including whether additional resources and/or activities would be necessary to effectively address these areas. The group also had detailed discussions on proposed changes to improve the effectiveness of the IS program and specific program office roles and responsibilities. One key area of discussion included whether to maintain the agency’s current decentralized approach, in which many NRC offices have IS responsibilities, or to propose a change to add a centralized IS activity management to integrate the separate IS functions. The ISSC concluded that centralized oversight was not necessary, but some efforts to integrate the various office IS activities, such as through the ISSC would have merit.

The group prioritized the identified areas for improvement according to their potential impact on achieving the NRC’s strategic objectives. The enclosed draft NRC Fiscal Year 2010–2015 ISSP, modeled after the Information Technology/Information Management Strategic Plan, lists the high-priority areas for improvement that the steering committee determined the NRC should address in the relatively near term (i.e., next 5 years). The ISSC acknowledged that the staff has several activities already underway (or recently completed) to address many of the high-priority areas for improvement. Examples of these activities include the power reactor security rulemaking (and new cyber security requirements under Title 10 of the *Code of Federal Regulations* Section 73.54, “Protection of Digital Computer and Communication Systems and Networks”) and the associated regulatory guidance document, as well as the update of Management Directive 12.5, “NRC Automated Information Security Program.” Should any new, emergent areas for improvement be identified, the ISSC intends to re-assess these high-priority items to ensure that the agency addresses the most critical IS areas first.

The IS program goals are as follows:

- IS Requirements, Standards, and Guidance—Ensure that IS requirements, standards, and guidance are clear, concise, appropriate, and able to mitigate the potential adverse effects if sensitive information is compromised

- IS Licensing, Approvals, and Inspection—Ensure that security controls for information owned by, or under the control of the NRC are consistent with established IS controls; that security controls for information are operating as intended; and that they are having the desired impact. Ensure similar controls for licensees regulated by the NRC are in compliance with NRC IS regulations.

- IS Enforcement and Allegation Processing—Ensure that suspected or actual IS violations are evaluated and appropriate sanctions are considered

- IS Emergency Preparedness and Incident Response—Ensure that the NRC has made sufficient preparations for IS-related emergencies and incidents

- Integrated IS Program—Ensure internal IS program components complement each other and are periodically evaluated and improved

ISSP Appendix Section A.3, “Situation Assessment,” contains a more comprehensive listing of the identified areas for improvement, together with proposed resolution strategies.

The purpose of the ISSP is to provide the NRC with an IS vision, and to establish a comprehensive IS program that focuses on attaining that vision, by describing strategies for strengthening the agency’s overall IS capabilities. The ISSP outlines a strategic approach for planning, prioritizing, and decision making, and it is aligned with and directly supportive of the NRC Strategic Plan (ADAMS Accession No ML072080203). The plan describes the contribution of NRC’s IS program activities to the agency’s overall mission to protect the health and safety of the public. It provides high-level direction to aid in the prioritization of the various NRC IS activities associated with IS oversight, including requirements and guidance development, security plan licensing and approval, inspection, investigations, enforcement, allegation processing, and emergency preparedness/incident response.

Consistent with the approach by which the NRC obtains feedback on its Strategic Plan updates, the staff intends to seek external stakeholder comment on the draft ISSP. In addition to making the document available for comment on the agency’s external website, the staff will consider conducting a public meeting to elicit feedback and to answer questions about how the ISSP was developed, and in what ways it will be used to guide agency decision-making. The staff anticipates issuing the ISSP in final form by the end of calendar year 2009.

Offices and staff with IS responsibilities should use the ISSP to aid the identification and prioritization of their IS-related work. The ISSC will revise the plan when it determines that a revision is needed, or at least once every 3 years.

COMMITMENT:

Listed below are the actions or activities committed to by the staff in this paper:

1. NRC will share the ISSP with external stakeholders for 30 days to receive comments.
2. Staff will revamp ISSP accordingly and inform the Commission if there are any notable changes.
3. The ISSC will review the ISSP at least once every 3 years and make necessary changes as warranted.

RESOURCES:

Some of the strategies in the ISSP can be implemented within existing agency resources since they summarize activities already being addressed by the offices represented on the ISSC. There are some activities, such as the assessment team for evaluating emergent cyber issues, that will be developed and pursued using the NRC's planning, budgeting and performance management process.

COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objection.

The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections.

/RA Darren B. Ash for/

R. W. Borchardt
Executive Director
for Operations

Enclosure:
As stated

U.S. Nuclear Regulatory Commission Fiscal Year 2010–2015 Information Security Strategic Plan

May 18, 2009

Enclosure

This page intentionally left blank.

May 18, 2009

A Message from the Deputy Executive Directors for Reactor and Preparedness Programs and Corporate Management

Statement to be added prior to final issuance.

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

1. Introduction

The U.S. Nuclear Regulatory Commission's (NRC's) Information Security Strategic Plan (ISSP) for Fiscal Year (FY) 2010–2015 describes how the information security (IS) program contributes to the agency's mission and provides high-level direction and prioritization for NRC internal IS activities and provides strategies to support NRC programs for oversight of licensee programs for information security control. The IS program addresses activities in the following areas: requirements and guidance, licensing and approval, inspection, enforcement, allegation processing, and emergency preparedness and incident response.

Section 1 covers the NRC's mission and responsibilities, the purpose of this plan, and its relationship to other planning documents. Section 2 discusses the planning outcomes, which are the IS program objective, vision, and strategic goals. Section 3 provides the strategies and measures associated with each of the goals. Section 4 describes the relationship of the IS strategic planning process to other agency planning processes and to the Federal program. Appendix A provides the context for this plan.

1.1 About the NRC

The Energy Reorganization Act of 1974 established the NRC to regulate the civilian use of nuclear materials for commercial, industrial, academic, and medical purposes. The NRC's mission is to do the following:

> License and regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment.

The NRC is responsible for licensing and regulating commercial nuclear power plants; research, test, and training reactors; nuclear fuel cycle facility licensees and certificate holders; medical, academic, and industrial uses of radioactive materials; and the transport, storage, and disposal of radioactive materials and wastes. The NRC's regulations are designed to protect the public and occupational workers from radiation hazards in those industries using radioactive materials. For more information about the NRC's activities, see http://www.nrc.gov.

1.2 The NRC Information Security Strategic Plan

The NRC's definition of IS is (1) protecting NRC and licensee information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction; (2) protecting electronic control functions from unauthorized access or manipulation; and (3) ensuring that adequate controls for protecting security-related information are used in the conduct of NRC business, both internal and external to the agency. The ISSP describes the NRC's strategy for strengthening its capabilities across all aspects of the IS program. This plan provides a strategic approach for planning and decision making and focuses on all types of activities closely related to IS, including but not limited to: (1) physical and environmental security, (2) personnel security, (3) classification management, (4) documentation, (5) systems, (6) telecommunications, (7) embedded information, (8) intelligence information, and (9) cyber-terrorism in its various forms.

The purpose of this plan is to establish an IS vision and to focus the NRC's IS program on attaining that vision. IS involves: (1) ensuring that accurate information is available to those authorized to access the information when they need it and (2) protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction.

1.3 Relationship to Other Planning Documents

The IS plan is aligned with the NRC's overall Strategic Plan, the Information Technology (IT)/Information Management (IM) Strategic Plan, and the Performance Budget. A brief summary of each follows:

- NRC Strategic Plan

  The NRC Strategic Plan documents agency-level goals and strategies for meeting the agency's overall mission to enable the use and management of radioactive materials and nuclear fuels for beneficial civilian purposes in a manner that protects public health and safety and the environment, promotes the security of the nation, and provides for regulatory actions that are open, effective, efficient, realistic, and timely. The ISSP is consistent with the agency's Strategic Plan and focuses more specifically on the IS goals and strategies. Section 2.3 provides more information on the relationship between the two plans.

- NRC IT/IM Strategic Plan

  The NRC IT/IM Strategic Plan describes how the IT/IM staff manages agency information; employs IT to improve the productivity, effectiveness, and efficiency of agency programs; and enhances the availability and usefulness of information to all users inside and outside the NRC. The NRC ISSP is consistent with the IT/IM Strategic Plan and focuses more specifically on the IS goals and strategies.

- NRC Performance Budget

  The NRC Performance Budget provides the proposed outcomes and measures associated with the funding needed to meet the agency's mission. Each year, the NRC submits its budget to the U.S. Office of Management and Budget (OMB) and, later, to the U.S. Congress. Beginning with the FY 2012 budget, which is expected to be submitted to OMB in fall 2010, the Performance Budget will consider the use of the targets for key measures laid out in Section 3 of the ISSP. As such, the NRC will align IS investments with the strategies and measures in the ISSP. The resource implications of the strategies and measures will be determined as part of the budget process when targets are set. Beginning with the FY 2012 budget cycle, the submittal will consider describing annual progress in achieving the IS program goals by reporting on the results for the key IS measures identified in Section 3.

2. IS Program Objective, Vision, and Strategic Goals

2.1 IS Objective and Vision

The box at the right shows the objective and vision of the NRC's agency-wide IS program. To accomplish an effective IS program, it is necessary to conduct oversight activities related to personnel security, physical and environmental security, IT security (cyber security), and non-IT IS. The NRC's IS activities include requirements development and maintenance, guidance development and maintenance, licensing and approvals, inspection, enforcement and allegation processing, and emergency preparedness and incident response for information control at NRC and regulated entities.

The NRC IS Program

Objective: Ensure that a cost-effective, consistent, and risk-informed level of information security is employed in the use and management of information owned by, or under the control of NRC in all its forms internal to the NRC and that a sufficient level of information security is implemented by licensees regulated by the NRC external entities

Vision: Information is valid and accessible only to those who are authorized access while retaining appropriate protections

2.2 IS Strategic Goals

Consistent with the NRC Strategic Plan and the situation assessment discussed in APPENDIX A, the NRC has adopted five strategic goals for its IS program:

Goal 1: IS Requirements, Standards, and Guidance—Ensure that IS requirements, standards, and guidance are clear, concise, appropriate, and able to mitigate the potential adverse effects if sensitive information is compromised

Goal 2: IS Licensing, Approvals, and Inspection— Ensure that security controls for information owned by, or under the control of the NRC are consistent with established IS controls; that security controls for information are operating as intended; and that they are having the desired impact. Ensure similar controls for licensees regulated by the NRC are in compliance with NRC IS regulations.

Goal 3: IS Enforcement and Allegation Processing—Ensure that suspected or actual IS violations are evaluated and appropriate sanctions are considered

Goal 4: IS Emergency Preparedness and Incident Response—Ensure that the NRC has made sufficient preparations for IS-related emergencies and incidents

Goal 5: Integrated IS Program— Ensure internal IS program components complement each other and are periodically evaluated and improved

These goals will be used to guide the NRC IS activities and investment priorities.

2.3 Relationship to the NRC Strategic Plan

The IS program supports all of the elements of the NRC's overall Strategic Plan. Table 2-1 relates some specific elements of the ISSP to the agency's strategic goals and objectives for organizational excellence.

Table 2-1 Examples of How the ISSP Supports the NRC Strategic Plan

Goals and Organizational Excellence Objectives with Associated Strategies from the NRC Strategic Plan	Supporting Goals and Strategies from the ISSP
Safety—Develop, maintain, and implement licensing and regulatory programs for reactors, fuel facilities, materials users, spent fuel management, uranium recovery, and decommissioning activities to ensure the adequate protection of public health and safety and the environment (Strategy 1) Security—Use relevant intelligence information and security assessments to maintain realistic and effective security requirements and mitigation measures (Strategy 1)	IS Requirements, Standards, and Guidance—Determine whether additional IS regulatory requirements or policies are needed for NRC-regulated entities based on changes to the threat environment or the enactment of new laws (1.4) IS Licensing, Approvals, and Inspection—Continue to ensure the security controls that protect licensees' sensitive information and IT systems that may directly or indirectly affect public safety and security meet regulatory requirements and are appropriately implemented (2.2)
Safety—Effectively respond to events at NRC-licensed facilities and other events of national interest, including maintaining and enhancing the NRC's critical incident response and communication capabilities (Strategy 9) Security—Share security information with appropriate stakeholders and international partners (Strategy 2)	IS Emergency Preparedness/ Incident Response— Communicate available IS threat information within NRC and to licensees to enable those affected to implement appropriate response/preparedness actions (4.1) Integrated IS Program—Enhance the ability to communicate securely and share sensitive information with internal and appropriate external stakeholders (5.2)
Safety—Review and refine an enforcement framework that emphasizes the importance of compliance with regulatory requirements and encourages prompt identification and comprehensive correction of licensee violations [Supports Strategy 8.] Security—Conduct inspections to assess licensees' security performance. The NRC will conduct follow up reviews, inspections, or investigations as needed when security problems are identified [Supports Strategies 2, 3, and 6]	IS Enforcement and Allegation Processing—Ensure NRC process for inspecting and documenting suspected IS violations by licensees is effective (3.1)
Openness—Provide for fair, timely, and meaningful stakeholder involvement in NRC decision making without disclosing classified, safeguards, proprietary, or sensitive unclassified information (Strategy 3)	IS Requirements, Standards, and Guidance—Update the NRC's internal IS security requirements, standards, guidance, and training to address current Federal guidance and changes in the threat environment (1.1) IS Licensing, Approvals, and Inspection—

Goals and Organizational Excellence Objectives with Associated Strategies from the NRC Strategic Plan	**Supporting Goals and Strategies from the ISSP**
	Strengthen the security controls that protect the sensitive information within NRC's control (2.1) Integrated IS Program—Establish an IS exchange forum for NRC IS oversight offices (5.3)
Effectiveness—Continue to improve the NRC's regulatory and communication programs (Strategy 7)	IS Licensing, Approvals, and Inspection—Continue to ensure the security controls that protect licensees' sensitive information and IT systems that may directly or indirectly affect public safety and security meet regulatory requirements and are appropriately implemented (2.2)
Operational Excellence—Manage agency information and employ IT to improve the productivity, effectiveness, and efficiency of agency programs and enhance the availability and usefulness of information to all users inside and outside the agency (Strategy 4)	IS Requirements, Standards, and Guidance—Develop and implement an internal NRC information security architecture (1.2) IS Licensing, Approvals, and Inspection—Strengthen the security controls that protect the sensitive information within NRC's control (2.1) Integrated IS Program—Establish a permanent IS steering committee (ISSC) to guide the NRC IS program (5.1)

3. Strategies and Performance Measures by Goal

This section establishes a set of strategies and measures for achieving each of the IS strategic goals. It provides examples of the means to execute each of the strategies that support each IS goal, followed by a brief discussion of the measures for each goal. Each year during the agency budget formulation process, the NRC will use these goals as input to considerations in allocating resources for implementing the strategies and set specific performance targets for each measure.

3.1 Goal 1: Information Security Requirements, Standards, and Guidance

IS Requirements, Standards, and Guidance: Ensure that IS requirements, standards, and guidance are clear, concise, appropriate, and able to mitigate the potential adverse effects if sensitive information is compromised

Strategies	Performance Measures
1. Update the NRC's internal IS security requirements, standards, guidance, and training to address current Federal guidance and changes in the threat environment	Update NRC Requirements, Standards, Guidance, and Training—80% of changes in Federal guidance are reflected in NRC requirements, standards, guidance and training within 12 months and all within 24 months IT Security Awareness Training—IT security awareness courses are updated to reflect internal IS security requirements and guidance within 12 months of their update. Role-Based IS Training— IT security role-based training courses are updated to reflect internal IS security requirements and guidance within 12 months of their update.
2. Develop and implement an internal NRC information security architecture	Enterprise Architecture—Percentage of IT implementations that comply with the Enterprise Architecture Security Architecture—Percentage of information security implementations that comply with the information security architecture
3. Incorporate IS guidelines into IT acquisition, implementation, and O&M requirements	IT Security Contract Language—New IT contracts and contract modifications incorporate information security contract language within 12 months of issuance. IS guidelines—IS guidelines for IT acquisition, implementation, and O&M developed within 12 months and implemented within 24 months

Strategies	Performance Measures
4. Determine whether additional IS regulatory requirements or policies are needed for NRC-regulated entities based on changes to the threat environment or the enactment of new laws	Update NRC IS Regulations, Standards, Guidance, and Training Applicable to Licensees—95% of changes in Federal guidance and threat environment are evaluated for placement in NRC requirements, standards, guidance and training within 12 months of issuance and all within 24 months of issuance.

Strategy 1—Update the NRC's IS security requirements, standards, guidance, and training to address current Federal guidance and changes in the threat environment

The NRC will update existing IS security directives, rules, and practices to ensure they address current Federal guidance and changes that have occurred in the threat environment. In addition, the NRC will develop new IT security standards to ensure a consistent application of IT security controls across implementations. The NRC will continue using awareness courses and will expand current role-based training to include all IS roles.

The NRC will update management directives for IT security, SUNSI security, and SGI security to include the new Federal guidance for controlled unclassified information.

Strategy 2—Develop and implement an internal NRC information security architecture

The NRC will develop, document, and implement a security architecture for NRC's IT systems. The IT security architecture will ensure identification of appropriate IS products and solutions to meet NRC's business needs while minimizing the operations and maintenance burden to the agency. As part of the IT security architecture, the NRC will develop formal procedures for introducing new technologies and products into the security architecture.

Strategy 3—Incorporate IS guidelines into IT acquisition, implementation, and O&M requirements

The NRC will enhance the information security guidelines as a part of IT acquisition, implementation, and O&M requirements. The enhanced formal process will include requirements for the initiation of IT acquisition, implementation, and O&M efforts, with requirements for approval and coordination related to Information Security. All requests for IT efforts will be required to conform to the Enterprise Architecture and security architecture and will only be accepted into the process if all required materials are complete and conform to the standards. The ITSAC will approve the formal IT process.

Strategy 4— Determine whether additional IS regulatory requirements or policies are needed for NRC-regulated entities based on changes to the threat environment or the enactment of new laws

The NRC will examine whether additional IS-related regulations and guidance are needed as new government-wide laws are enacted or as threat conditions change. Cognizant NRC management, in consultation with CSO and other Federal stakeholders (as appropriate), will identify needed IS training to provide the NRC staff with the knowledge, skills, and abilities to effectively license facilities and inspect digital control systems and network applications at licensee facilities.

Measures for Goal 1

The NRC is adopting eight measures to monitor progress in achieving the major elements of the IS requirements, standards, and guidance goal. The measures are intended to strengthen IS controls for NRC information and areas regulated by the NRC.

3.2 Goal 2: Information Security Licensing, Approvals, and Inspection

IS Licensing, Approvals, and Inspection: Ensure that security controls for information owned by, or under the control of the NRC are consistent with established IS controls; that security controls for information are operating as intended; and that they are having the desired impact. Ensure similar controls for licensees regulated by the NRC are in compliance with NRC IS regulations.

Strategies	Performance Measures
1. Strengthen the security controls that protect the sensitive information within NRC's control	System Certification and Accreditation—90% of major applications and general support systems have been certified and accredited for internal NRC IS IS Controls—90% of identified IS control issues closed within the plan of action and milestones agreed upon timeframe FISMA Compliance Process Effectiveness—Rating of the NRC's FISMA compliance and continuous monitoring process based on the annual IG assessment
2. Continue to ensure the security controls that protect licensees' sensitive information and IT systems that may directly or indirectly affect public safety and security meet regulatory requirements and are appropriately implemented	Security Control Review—Update the Standard Review Plan for licensee applications, upgrades, renewals, and inspection guidance to include a review of IS controls that may directly or indirectly affect public safety, as appropriate to the review or inspection within 12 months of issuance. Verify Facility and Personnel Security Clearances Granted by Other Government Agencies— 99% of the time, facility and personnel clearances can be verified in sufficient time to support the timely exchange of information among authorized stakeholders with a need to know

Strategy 1—Strengthen the security controls that protect the sensitive information within NRC's control

The NRC will ensure adequate resources for the IS program and will improve the effectiveness and efficiency of the NRC IS approval and inspection process for internal IS. The revised process will promote a better understanding of enterprise-wide mission risks resulting from the NRC's information management processes and the operation of information systems and improve the security of the NRC's sensitive information, whether in electronic or hard-copy form.

ADM will develop a formal inspection process to determine if SUNSI, SGI, and NSI documents are being properly protected within NRC. The process will use the associated management directives to identify the requirements for protection. In addition, CSO will develop a formal IT security inspection process for all NRC systems, as well as for IT devices that enter NRC facilities.

Strategy 2—Continue to ensure the security controls that protect licensees' sensitive information and IT systems that may directly or indirectly affect public safety and security meet regulatory requirements and are appropriately implemented

The NRC will continue to ensure that licensees' IS controls are in keeping with established requirements, and that licensees periodically assess the continued effectiveness of their IS controls as new threats arise or vulnerabilities are identified.

Measures for Goal 2

The NRC is adopting five measures to monitor progress in achieving the major elements of the IS Licensing, Approvals, and Inspection goal. The measures are intended to strengthen NRC's internal IS controls of sensitive information, and to enhance the NRC's oversight of licensees' compliance with established IS requirements.

3.3 Goal 3: Information Security Enforcement and Allegation Processing

IS Enforcement and Allegation Processing: Ensure that suspected or actual IS violations are evaluated and appropriate sanctions are considered

Strategies	Performance Measures
1. Ensure NRC process for inspecting and documenting suspected IS violations by licensees is effective	Licensee IS Violation Inspection—Inspectors are trained on the Standard Review Plan for Licensee applications, upgrades, renewals, and inspection guidance to include a review of IS controls that may directly or indirectly affect public safety, as appropriate to the review or inspection prior to the effective date of any new IS requirements
2. Clarify regulatory tools to ensure that they adequately address IS and cyber security	Identify licensee consequences—Enforcement Policy Supplements are updated to include

Strategies	Performance Measures
enforcement	examples of IS violations within 12 months after issuance of this plan or prior to the effective date of new requirements, whichever comes later.

Strategy 1—Ensure NRC process for inspecting and documenting suspected IS violations by licensees is effective

The inspection staff will receive IS training in new inspection procedures and Part 73 requirements and will obtain feedback on effectiveness of inspections during the first year of procedural use.

Strategy 2—Clarify regulatory tools to ensure that they adequately address IS and cyber security enforcement

The NRC will update and communicate a shared understanding of specific enforcement actions that will be taken to licensees for noncompliance with IS requirements.

Measures for Goal 3

The NRC is adopting two measures to monitor progress in achieving the major elements of the IS Enforcement and Allegation Processing goal. The measures are intended to improve IS at licensee facilities.

3.4 Goal 4: Information Security Emergency Preparedness and Incident Response

IS Emergency Preparedness and Incident Response: Ensure that the NRC has made sufficient preparations for IS-related emergencies and incidents

Strategies	Performance Measures
1. Communicate available IS threat information within NRC and to licensees to enable those affected to implement appropriate response/preparedness actions	IS Threat Information—Within 12 months of issuance of this plan, NRC has established and implemented a process to obtain applicable IS threat information from the intelligence community and communicate that information to appropriate licensees.
2. Establish a cyber issue assessment process and a cyber assessment team to address licensee cyber security issues	Cyber Issue Assessment Process—Within 6 months of issuance of this plan, Cyber Issue Assessment Process, Rev 0, is approved and implemented. Cyber Assessment Team—90% of issues reviewed by the Cyber Assessment Team are

Strategies	Performance Measures
	closed or transferred to another process (e.g., generic communications) within 60 days of identification. Cyber Security Effectiveness—No events meeting abnormal occurrence criteria result from malicious cyber activity.
3. Update NRC internal emergency response plans and procedures to reflect current IS practices and the current threat environment	Emergency Response Plans and Procedures—Emergency response plans for IS events are reviewed annually for conformance to current IS practices, guidance and changes in the threat environment. Emergency Response Plan Updates—Revisions or updates deemed necessary to comport with current practices or guidance or to mitigate changes in the threat environment are implemented within 12 months.

Strategy 1— Communicate available IS threat information within NRC and to licensees to enable those affected to implement appropriate response/preparedness actions

The NRC will subscribe to available services that provide IT security threat advisories using existing interagency connections and networks. The staff will identify, categorize, characterize, prioritize, and communicate IT security threats and vulnerabilities of potential impact to the agency and licensees and will identify and communicate appropriate countermeasures.

Strategy 2—Establish a cyber issue assessment process and a cyber assessment team to address licensee cyber security issues

The NRC has developed a licensee cyber issue assessment process for the evaluation and resolution of identified cyber-related security issues and potential or actual cyber-related security threats. A cyber assessment team is being staffed by the various responsible offices to evaluate and assess licensee cyber issues and support NRC organizations in effectively addressing the issues.

Strategy 3—Update NRC internal emergency response plans and procedures to reflect current IS practices and the current threat environment

The NRC will update its emergency response plans and procedures to include information needed to maintain continued operation, given a malicious event.

Measures for Goal 4

The NRC is adopting six measures to monitor progress in achieving the major elements of the IS Emergency Preparedness and Incident Response goal.

3.5 Goal 5: Integrated Information Security Program

Integrated IS Program: Ensure internal IS program components complement each other and are periodically evaluated and improved

Strategies	Performance Measures
1. Establish a permanent IS steering committee (ISSC) to guide the NRC IS program	ISSC—ISSC Charter is revised within 3 months of issuance of this plan
2. Enhance the ability to communicate securely and share sensitive information with internal and appropriate external stakeholders	Secure Communication with Stakeholders—Within 24 months of issuance of this plan and Commission approval of an approach and associated budget, the NRC staff can securely communicate sensitive information with key stakeholders
3. Establish an IS exchange forum for NRC IS oversight offices	IS Exchange Forum—Annual stakeholder survey of effectiveness of communications to identify and implement continuous improvement activities

Strategy 1—Establish a permanent IS steering committee to guide the NRC IS program

The NRC will continue using the ISSC to guide its IS program. The NRC will modify the composition and charter of the ISSC to match agency needs and establish working groups to address concerns as they arise.

Strategy 2—Enhance the ability to communicate securely and share sensitive information with internal and appropriate external stakeholders

The NRC will enhance the ability of its staff to securely communicate sensitive information with stakeholders.

Strategy 3—Establish an IS exchange forum for NRC IS oversight offices

The NRC will establish a forum to facilitate the exchange of IS information among NRC offices with IS oversight responsibilities. The forum will enable cross-training and provide a method of disseminating information in a timely manner.

Measures for Goal 5

The NRC is adopting three measures to monitor progress in achieving the major elements of the Integrated IS Program goal. Each element has a single measure.

4. IS Strategic Planning and Performance Measurement Process

In FY 2008, the NRC initiated an IS strategic planning process and requested participation from all offices with IS oversight responsibilities. Subsequently, the ISSC was established to enhance executive leadership involvement in the process. As a result, the NRC established an ISSP working group to gather information about IS oversight activities and the roles and responsibilities associated with each activity. At the direction of the ISSC, the working group organized and summarized the detailed information it had collected into the first draft of the ISSP, with the anticipation that a revision will be required after the first year of use. The ISSC, the Deputy Executive Director for Reactor and Preparedness Programs (DEDR), the Deputy Executive Director for Corporate Management (DEDCM), and the Executive Director for Operations (EDO) reviewed and approved this plan.

4.1 Description of the IS Planning and Performance Measurement Process

The IS strategic planning and performance measurement process consists of the following 10 steps:

(1) identify strengths, weaknesses, opportunities, and threats (SWOT) through an external and internal assessment;

(2) use a strategic analysis to identify and prioritize major issues and goals;

(3) design major strategies to address issues and goals;

(4) design and update the vision, mission, and values;

(5) establish action plans (strategies, resource needs, roles, and responsibilities for implementation);

(6) record issues, goals, strategies, programs, updated mission and vision, and action plans in a strategic planning document and attach a detailed analysis of strengths, weaknesses, opportunities, and threats, resource needs, and other issues;

(7) develop the yearly operating plan document (from year one of the multiyear strategic plan);

(8) develop and authorize the budget for year one (allocation of funds needed to fund year one);

(9) conduct the organization’s first-year operations; and

(10) monitor, review, evaluate, and update the ISSP.

4.2 Relationship to Other Planning and Performance Measurement Processes

The NRC framework for performance-based management is the Planning, Budgeting, and Performance Management process that was established in January 1998 and updated in July 2002. This process implements the Government Performance and Results Act, which requires the submission of a Strategic Plan, Performance Budget, and Performance Report to

Congress. The NRC has designed the new IS strategic planning process to be an integral part of the agency's Planning, Budgeting, and Performance Management process.

Annually, the Commission provides guidance on the outcome-based performance measures, which indicate the level of success needed to achieve the agency's goals. The performance measures form the basis for the NRC to develop key planning assumptions, which identify major program drivers that would significantly influence the NRC's work activities and resource requirements. For each major activity, the agency identifies the major program outputs and output-based measures needed to achieve the outcome-based performance measures, taking into consideration the key planning assumptions. The NRC also identifies and prioritizes planned activities, including those for IS, needed to achieve the outputs in each major activity and then prioritizes them based on their contribution to the goals. Lastly, the NRC determines the resource requirements needed to achieve each planned activity, which form the basis for developing the agency's budgetary requests for each program area. At each performance budget review level, the NRC takes into consideration those factors described above in relating outcome-based and output-based performance measures to resources to make budget recommendations and decisions.

4.3 Roles and Responsibilities for IS Strategies and Measures

The NRC's DEDR and the DEDCM have overall responsibility for the IS strategic planning process. In addition, the ISSC provides direction to and oversight of the IS strategic planning effort. The ISSC has senior executive representation from the organizations that have IS oversight responsibilities, including mission offices. The senior executive representatives are responsible for working with representatives of other relevant NRC organizations to develop tactical plans for implementing strategies and measures. The responsible senior executives must also track the strategy or measure across the agency and report results during the annual IS performance review. The DEDR and the DEDCM guide the ISSC, direct the overall implementation of the plan, ensure coordination among strategy stakeholders, and track progress of the measures for use in performance reviews.

APPENDIX A IS ENVIRONMENT AND CONTEXT

This section provides a high-level summary of the areas and consideration factored into the development of the ISSP, the IS program management approach, the environment in which the IS program operates, the strengths of the program, and areas for improvement.

A.1 The NRC Strategic Plan

The NRC Strategic Plan forms the foundation for IS strategic planning by identifying the NRC's overall strategic direction for the planning period. The plan explains the vision, strategic objectives, strategic goals, associated outcomes, and organizational excellence objectives.

Strategic Goals and Outcomes:

Safety: Ensure adequate protection of public health and safety and the environment.

- Prevent the occurrence of any nuclear reactor accidents.
- Prevent the occurrence of any inadvertent criticality events.
- Prevent the occurrence of any acute radiation exposures resulting in fatalities.
- Prevent the occurrence of any releases of radioactive materials that result in significant radiation exposures.
- Prevent the occurrence of any releases of radioactive materials that cause significant adverse environmental impacts.

Security: Ensure adequate protection in the secure use and management of radioactive materials.

- Prevent any instances in which licensed radioactive materials are used domestically in a manner hostile to the United States.

The full text of the NRC's Strategic Plan may be found at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1614/. The goals and strategies in this IS plan contribute both to the safety and security goals and to the organizational excellence objectives in the agency's strategic plan.

A.2 The NRC IS Program Management Approach

The EDO is responsible for the NRC's IS program, as directed by the Commission. Offices that report directly to the Commission and offices that report to the EDO execute the program. The NRC has a wide variety of IS responsibilities and uses a matrix management approach to ensure the right skills are available to address IS needs.

A.2.1 Information Security Component Description

This section describes the different components of the NRC's IS program.

Information Security Oversight Activities

The NRC's IS oversight activities for both internal NRC IS and external regulation[1] of licensees include the following:

- Requirements Development and Maintenance
  - This activity involves the establishment and maintenance of directives, regulations, license conditions, certificate conditions, and orders.
- Guidance Development and Maintenance
  - This activity involves creating and maintaining guidance related to IS requirements, to determine whether individuals or regulated entities comply with requirements, as well as providing training to help people and organizations understand their responsibilities.
- Licensing and Approvals
  - This activity involves actions required to determine whether to approve or license an activity or work product, as well as the licensing or approval action resulting from the determination.
- Inspection
  - This activity involves actions taken to determine if licensees are following regulations and other legal requirements.
- Enforcement and Allegation Processing
  - This activity involves actions taken to emphasize the importance of compliance with requirements and to encourage prompt identification and resolution of violations, as well as actions taken in response to a declaration, statement, or assertion of impropriety or inadequacy associated with NRC requirements, the validity of which has not been established.
- Emergency Preparedness and Incident Response
  - This activity involves actions to prepare for a potential emergency or incident, develop associated plans, train individuals on the proper response to an emergency or incident, and respond to incidents.

The following NRC offices perform "internal" IS oversight:

- The Office of Administration (ADM) performs physical, environmental, and personnel security activities.
- The Computer Security Office (CSO) performs IT (cyber) security activities.

[1] Note that these are not part of formal IS oversight activities but are parts of the program office's oversight of regulated entities.

- The Office of the General Counsel (OGC) performs legal support activities.
- The Office of Information Services (OIS) performs non-IT Sensitive Unclassified Non-Safeguards Information (SUNSI), Privacy Act (PA), Freedom of Information Act (FOIA), and records management activities.
- The Office of Nuclear Security and Incident Response (NSIR) performs non-IT Safeguards Information (SGI) and classified National Security Information (NSI) activities.

"External" IS oversight activities are part of regulatory programs for entities regulated by the NRC and are performed by the following organizations:

- ADM performs personnel security activities.
- The Atomic Safety and Licensing Board Panel (ASLBP) determines information handling requirements for adjudicatory hearings.
- The Office of Federal and State Materials and Environmental Management Programs (FSME) performs regulatory activities pertaining to industrial, academic, and medical uses of radioactive materials; Agreement States; uranium recovery fuel cycle licensees; and decommissioning nuclear power reactors, non-power reactors, and complex materials sites.
- OGC performs legal support activities.
- The Office of Nuclear Material Safety and Safeguards (NMSS) perform regulatory activities pertaining to fuel cycle facilities, spent fuel storage and transportation, and high-level waste (HLW) repositories.
- The Office of Nuclear Reactor Regulation (NRR) performs regulatory activities pertaining to operating nuclear power reactors and non-power reactors.
- The Office of New Reactors (NRO) performs regulatory activities pertaining to new nuclear power reactors.
- The Office of Nuclear Security and Incident Response (NSIR) performs security, emergency preparedness, and incident response-related regulatory activities pertaining to nuclear power reactors; fuel cycle facilities; independent spent fuel storage installations; spent fuel storage and transportation; industrial, academic, and medical users of radioactive materials; HLW repositories; and power reactor vendors.
- The Office of Enforcement (OE) performs regulatory enforcement activities.
- The Office of Investigations (OI) performs regulatory investigation activities.
- Regional offices (REGIONS) perform regulatory activities pertaining to licensees, such as nuclear power reactors, non-power reactors, fuel cycle facilities, Agreement States, and materials facilities.

Information Security Oversight Categories

Each IS oversight activity (e.g., requirements development and maintenance) can be further divided into four categories, as follows:

(1) Personnel Security

- This includes the NRC reviews and eligibility determinations for access to controlled information, SGI, NSI, and sensitive NRC IT systems or data; for example, determining whether an individual may receive and review certain types of SUNSI, SGI, Restricted Data, and NSI, under the NRC's control.

(2) Physical/Environmental Security

- This includes granting and terminating NRC clearances for specific secure NRC facilities, or licensee facilities, designating and terminating physical protection facilities within the NRC, and surveying these facilities and license facilities to ensure compliance with security standards, as well as physical and environmental security requirements as they pertain to the protection of information; for example, determining whether SUNSI, SGI, and NSI documents and reports are physically protected from unauthorized disclosure.

(3) IT (Cyber) Security

- This includes protection of the confidentiality, integrity, authenticity, and availability of electronic information, as well as protection from unauthorized access to instrumentation and control functions related to safety, security, and emergency preparedness within NRC facilities and licensing and inspecting licensee facilities for adequate control. For example—

    ▪ determining whether an NRC system complies with the configuration standards for the operating system, applications, and interface controls

    ▪ determining, through licensing and inspection activities, whether computer-based systems within a nuclear facility affecting safety or security will not be affected by unauthorized access.

(4) Non-IT IS

- This category includes the protection of SUNSI, SGI, and NSI, including the confidentiality, integrity, authenticity, and availability of offline data, when the information is not in electronic form.

A.2.2 Information Security Roles and Responsibilities

This section describes the organizational roles and responsibilities associated with NRC internal IS oversight and summarizes the IS support for NRC offices with oversight of licensee activities as part of each aspect of the NRC's regulatory mission (i.e., requirements development, rulemaking and guidance development, licensing, inspection, enforcement, allegation processing, emergency preparedness and incident response).

Requirements and Guidance Development and Maintenance

Various NRC offices develop and implement IS-related requirements, with Commission approval (as necessary). Once the NRC establishes IS requirements, it communicates them to its staff and contractors and provides guidance and training to assist in implementation. The NRC issues IS requirements related to or affecting NRC licensees by means of rules, orders, generic communications, and license or certificate conditions that must be followed, and supplements these requirements with guidance documents (e.g., NUREGs) to aid in implementation.

The NRC establishes Internal IS requirements and guidance in management directives, handbooks, yellow announcements, regulations, and other documents. The following NRC offices have internal IS requirements and guidance responsibilities:

ADM: NRC personnel security and physical and environmental security

CSO: NRC IT (cyber) security

NSIR: NRC non-IT IS for SGI and NSI

OGC: Legal support on all matters

OIS: NRC non-IT IS for SUNSI information

External IS requirements are established by regulations and licensee conditions for licensees regulated or overseen by the NRC. The following NRC offices have external IS requirements and guidance responsibilities:

FSME & Region Offices: Personnel security, physical and environmental security, IT security, and non-IT IS for industrial, academic, and medical users of radioactive materials; uranium recovery fuel cycle licensees; decommissioning nuclear power reactors, non-power reactors, and complex materials sites; and Agreement States

NMSS & RII: Personnel security, physical and environmental security, IT security, and non-IT IS for fuel cycle facilities

NRR & Region Offices: Personnel security, physical and environmental security, IT Security, and non-IT IS for power reactors and research and test reactors

NSIR: Personnel security, physical and environmental security, IT security, and non-IT IS for power reactors, fuel cycle facilities, independent spent fuel storage installations, spent fuel storage and transportation certificate holders, and power reactor vendors

OGC: Legal support on all matters

NRO & Region Offices IT security and non-IT security for new and advanced reactors applicants, licensees, and vendors

Licensing and Approvals

The NRC conducts reviews of information handling and processing procedures internal to the NRC (and provides approvals as appropriate). Approvals occur in many forms, such as system accreditation, acceptance of the security implications of a specific system modification, granting access to NSI, or issuance of a facility badge.

The NRC issues a license or certificate that includes external IS activities when an applicant demonstrates the ability to meet the applicable regulatory requirements. Under the Atomic Energy Act of 1954, as amended, Section 274i, States may perform this function for certain types of licensees.

The NRC conducts internal IS reviews to approve or disapprove the use of IT systems or devices and modifications to those systems and devices. The following NRC offices provide internal IS approval:

ADM: NRC personnel security and physical and environmental security

CSO: NRC IT (cyber) security

OGC Legal support on all matters

NSIR & Region Offices: NRC non-IT IS for SGI and NSI

OIS: NRC non-IT IS for SUNSI information

The NRC staff conducts external licensing reviews when entities submit information to the NRC to obtain a license or request a license change. For example, licensing reviews may include the determination of whether the proposed use of supervisory control and data acquisition systems in a commercial power reactor facility comply with NRC regulations. The following NRC offices provide external IS licensing and approvals (to include IS):

ADM: NRC personnel security for nuclear power reactors; fuel cycle facilities; independent spent fuel storage installations; spent fuel storage and transportation certificate holders; industrial, academic, and medical users of radioactive materials; HLW repositories; power reactor vendors; State and Tribal programs and Agreement States

FSME: Personnel security, physical and environmental security, IT security, and non-IT IS for industrial, academic, and medical users of radioactive materials; uranium recovery fuel cycle licensees; decommissioning nuclear power reactors, non-power reactors, and complex materials sites; and Agreement States.

NMSS: IT security, and non-IT IS for fuel cycle facilities

Personnel security, physical and environmental security, IT security, and non-IT IS for HLW repositories

NRR: Personnel security, physical and environmental security, IT security, and non-IT IS for power reactors and research and test reactors

NRO: IT security for new nuclear power reactor applicants, licensees, and vendors

NSIR & Region Offices: Input to and sometimes decisions on physical and environmental security, IT security, and non-IT IS for independent spent fuel storage installations; spent fuel storage and transportation certificate holders; industrial, academic, and medical users of radioactive materials; power reactor vendors

Input to and sometimes decisions on physical and environmental security and IT security for fuel cycle facilities and physical and environmental security for nuclear power reactors and HLW repositories

OGC: Legal support on all matters

Inspection

The NRC conducts inspections to determine if organizations and individuals meet its requirements. For internal NRC IS, inspections determine if the NRC staff and contractors are following agency requirements. The NRC oversees the Agreement State program and performs Integrated Materials Performance Evaluation (IMPEP) reviews of the Agreement States and the regions, which are similar to inspections of NRC licensees and certificate holders. The NRC uses inspections to determine if a licensee or certificate holder meets the applicable IS requirements.

Internal IS inspections determine if the NRC staff's IS activities are in compliance with established agency requirements. The following NRC offices conduct internal IS inspections:

ADM:	NRC personnel security and physical and environmental security NRC non-IT IS for SGI and NSI Foreign assignee security plans
CSO:	NRC IT (cyber) security
OGC:	Legal support on all matters
OIS:	NRC non-IT IS for SUNSI information

Similarly, the NRC conducts inspections at licensee facilities to determine whether applicable regulatory requirements are being met. The following NRC offices conduct external IS inspections:

FSME & Region Offices:	Personnel security, physical and environmental security, IT security, and non-IT IS for industrial, academic, and medical users of radioactive materials; uranium recovery fuel cycle licensees; decommissioning nuclear power reactors, non-power reactors, and complex materials sites; and Agreement States.
NMSS & RII:	Physical and environmental security for HLW repositories
NRO & RII:	IS security and non-IT IS for new power reactor applicants, licensees and vendors
NRR & Region Offices:	Personnel security, physical and environmental security, system level IT, and non-IT IS for power reactors and research and test reactors
NSIR:	IT security and non-IT IS for power reactors; fuel cycle facilities; independent spent fuel storage installations; spent fuel storage facilities and transportation certificate holders; industrial, academic, and medical users of radioactive materials; HLW repositories; power reactor vendors
OGC:	Legal support on all matters
Region Offices:	Personnel security, physical and environmental security, IT security, and non-IT IS for power reactors; fuel cycle facilities; independent spent fuel storage installations; spent fuel storage facilities and transportation certificate holders; industrial, academic, and medical users of radioactive materials; HLW repositories; power reactor vendors

Enforcement and Allegation Processing

The NRC uses enforcement measures to emphasize the importance of compliance with requirements and to encourage prompt identification and resolution of violations. Internally, enforcement may take the form of a warning or other disciplinary action against the NRC staff or, for a contractor, removal from NRC work. The NRC considers regulatory enforcement for its licensees when it identifies violations of regulatory requirements. Under the Agreement State program, the NRC can implement a wide range of actions to address findings, from increased frequency of IMPEP reviews to assuming the oversight program from the State.

Allegations are declarations, statements, or assertions of impropriety or inadequacy associated with NRC requirements, the validity of which has not been established. Internally, these may take the form of inappropriate actions (e.g., using another individual’s computer account, sharing information with someone not authorized to have the information, installing unauthorized software) and may be handled by line management or referred to the NRC Office of the Inspector General. For regulated entities, regulatory allegations assert wrongdoing by individuals or organizations that are (1) licensed by the NRC, (2) applicants for licenses, (3) licensee contractors or vendors, or (4) employees of (1), (2), or (3).

Internal IS allegation processing involves the investigation of allegations of wrongdoing or noncompliance with NRC requirements. Internal IS enforcement may involve disciplining the NRC staff for IS infractions. The following NRC offices provide internal IS enforcement and allegation processing:

ADM:	Issues notices of infractions for acts or omissions involving failure to comply with NRC security requirements or procedures for the protection of NSI Issues notices of infractions for failure to physically protect security information
OGC:	Legal support on all matters
All Program & Region Offices:	NRC Personnel Security and physical and environmental security, NRC non-IT IS for SGI and in some cases NSI

External IS regulatory allegation processing involves a formal review (and potential investigation) of all allegations. The NRC imposes a range of consequences for confirmed failures to meet established IS requirements. The following NRC offices provide external IS regulatory enforcement and allegation processing: FSME, NMSS, NRO, NRR, NSIR, OE, OGC, OI, and REGIONS.

Emergency Preparedness and Incident Response

Emergency preparedness involves taking actions necessary to prepare for incidents and emergencies. Incident response involves taking actions during or after an actual event.

Internal IS emergency preparedness and incident response involve taking actions to protect against the current threat model for IS security at the NRC and investigating potential compromises of NRC IS. The following NRC offices are responsible for internal IS emergency preparedness and incident response:

ADM: Develops, maintains, and implements the NRC Occupant Emergency Plan
Administers the NRC security infraction program
Responds to physical and environmental security incidents within NRC facilities

CSO: Leads NRC IT security incident response

NSIR: Serves as the Chief Infrastructure Assurance Officer and leads NRC Incident Response for SGI or NSI inspections.

OGC: Legal support on all matters

OIS: Supports NRC IT security incident response

Region Offices: Implement specific office Occupant Emergency Plans and lead NRC response to SGI or NSI infraction in that office.

External IS emergency preparedness and incident response involves ensuring that regulated entities have implemented measures and taken actions necessary to respond effectively to potential or actual IS compromises. The following NRC offices are responsible for external IS emergency preparedness and incident response: FSME, NRO, NRR, NSIR, OGC, and REGIONS.

A.3 Situation Assessment Performed by the ISSC Working Groups

The IS strategic planning process began with a situation assessment and a review of the NRC's role as it relates to the IS needs of NRC stakeholders. The assessment included an examination of the programmatic drivers for the NRC; drivers from external oversight; the political, economic, and technological environment; strengths of the NRC IS program; and areas for improvement. This section contains a summary of the results of this assessment.

The NRC's Stakeholders

The NRC's external stakeholders include the agency's licensees or certificate holders and their contractors, the nuclear industry, advocacy organizations, the Congress, OMB, State and local governments, Indian tribes, Native American Tribal Governments, other Federal agencies (such as the U.S. Department of Energy, the U.S. Department of Homeland Security (DHS), and the U.S. Environmental Protection Agency), international nuclear entities and nuclear regulators, academia, individuals living near regulated facilities, and the general public.

Internal stakeholders include the Commission, senior executives, managers, and staff. Each of these stakeholders has interests particularly relevant to IS planning, including the following:

- nuclear facility safety and security
- protection of the confidentiality of information that is not publicly available (including privacy information)
- protection of the integrity of NRC information
- access by external stakeholders to agency information needed to understand the NRC's mission, goals, and performance and to participate effectively in the regulatory process
- ability to communicate and share information (securely, as needed) internally and externally
- ability to conduct business effectively and efficiently, both internally and externally

Information Security Drivers

Agency programs and activity areas expected to be the main drivers for continued IS program development include the following:

NRC Programmatic Drivers

- the evolving threat environment
- new reactor, fuel facility, and HLW repository applications
- nuclear nonproliferation activities
- increased coordination with Federal partners, including the need for secure communications
- increased need for defense-in-depth IT infrastructure
- continued emphasis on the NRC's goal to ensure openness in its regulatory processes
- enhancements to the National Materials Program

External Oversight Drivers

- continued focus by oversight agencies on how federal agencies meet security and privacy requirements, including those in the Federal Information Security Management Act (FISMA)
- continued need for an effective response to Government-wide initiatives with significant IS implications, such as Homeland Security Presidential Directive 12 (HSPD-12) and Federal implementation of Internet Protocol Version 6 (IPv6)
- continued oversight focus from the National Archives and Records Administration and OMB to comply with Federal records laws and regulations under 44 U.S.C. 2901, 3101, and 3102, as well as OMB Circular A-130, "Management of Federal Information Resources," related to establishing and maintaining continuous and systematic control of information throughout its lifecycle
- continued DHS coordination of the Nuclear Reactors, Materials, and Waste Critical Infrastructure Protection Sector, including implementation of the Comprehensive National Cyber Security Initiative

Political Environment Drivers

- heightened concern about terrorism, the threat of a flu pandemic, and recent natural disasters
- increased emphasis on Federal continuity of operations
- search for new energy sources, including new nuclear power plants
- foreign country involvement in commercial uses of nuclear materials

Economic Environment and Workforce Drivers

- the Federal fiscal environment's provision of a strong impetus for process efficiencies
- higher energy prices, space limitations, and staff retention needs creating an increase in telecommuting
- growth in the nuclear industry, increasing turnover and competition for qualified staff

- shortage of needed IS skills and resulting competition for qualified staff
- growth in numbers of NRC staff, resulting in acquisition of leased space

Technological Environment Drivers

- technology advances enabling work anywhere at anytime
- increased use of digital instrumentation and controls at nuclear facilities
- increased emphasis on the security of supervisory control and data acquisition systems within the critical infrastructure sectors
- challenges stemming from the need to preserve information during an era of rapid technological change and storage media obsolescence
- connectivity to Federal, State, and local partners, including SUNSI, SGI, and NSI networks
- foreign technology interchange

Strengths

To prepare for the IS situational assessment, the NRC staff reviewed recent performance self-assessments, OIG and U.S. Government Accountability Office (GAO) audits, and internal performance measures. The assessment also included surveys of representatives from the entire range of internal NRC organizations.

The review and survey identified the following NRC IS program strengths:

Internal

- CSO establishment, providing computer security oversight independence and additional resources
- improvements in the certification and accreditation process and an increase in the percentage of current NRC system accreditations
- specialization of personnel within a given area of IS expertise
- leadership and management by IS professionals
- dedication of staff
- synergy of many security skills (physical, technical, communications, personnel, and information management) within the NRC staff

External

- comprehensive non-IT SGI and NSI regulations
- strong IS program related to physical controls
- specialization of personnel within a given area of IS expertise
- leadership and management by security professionals
- dedication of staff
- intra-agency communications (i.e., among agency offices)

Recommended Areas for Improvement

The IS performance review also identified the following areas for potential improvement:

Internal

- agency wide understanding of IS and its role in achieving the NRC's overall mission
- continued coordination and collaboration among existing NRC IS and cyber security professionals
- IS role-based training for those with IS oversight responsibilities
- IS requirements, guidance, and standards updates to reflect current Federal guidance and the evolving threat environment
- Enterprise Architecture and security architecture implementation that enhances security controls
- formal process for IT acquisition, implementation, and O&M requirements that includes all NRC IT devices, software, and development that takes into account security needs
- availability of IT security threat advisories using existing interagency connections and networks; prioritization of IT security threats and vulnerabilities; implementation of appropriate corrective actions
- improvements in security controls that protect NRC sensitive information
- provide means for secure communications with stakeholders

External

- review of design-basis threat cyber attack threat characteristic
- development of cyber security program guidance for use by licensees and applicants and system-level cyber security guidance for safety-related instrumentation and control applications
- development of a cyber security inspection program
- communication of emergent cyber threat and vulnerability information to licensees
- development of IS guidance specific for vendors of digital systems and components for vendors of new reactor and fuel cycle facility designs
- collaboration with international entities regarding the development of standards, guidance, and oversight programs