OFFICE OF THE INSPECTOR GENERAL
U.S. NUCLEAR REGULATORY COMMISSION

Systems Evaluation of the
General License Tracking
System (GLTS)

OIG–04-A-24 September 30, 2004

EVALUATION REPORT

All publicly available OIG reports (including this report) are accessible through NRC's website at:
http://www.nrc.gov/reading-rm/doc-collections/insp-gen/

September 30, 2004

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: SYSTEM EVALUATION OF THE GENERAL LICENSE TRACKING SYSTEM (GLTS) (OIG-04-A-24)

This evaluation was conducted as part of the Office of the Inspector General's review of NRC's implementation of the Federal Information Security Management Act (FISMA) for FY 2004. Richard S. Carson & Associates, Inc., performed this independent system evaluation on behalf of OIG.

Based on its review and evaluation of the General License Tracking System's management, operational, and technical controls, Richard S. Carson & Associates, Inc., determined that GLTS has the following weaknesses:

- Security documentation for GLTS does not always follow required guidelines.
- Security protection requirements are inconsistent within GLTS' security documentation.
- NRC is not tracking all action items resulting from testing GLTS' security controls.

The weaknesses identified are not significant deficiencies or reportable conditions. During an exit conference on September 13, 2004, NRC officials provided comments concerning the draft audit report and opted not to submit formal written comments to this report.

If you have any questions or wish to discuss this report, please call me at 415-5915 or Beth Serepca at 415-5911.

Attachment: As stated

Distribution List

B. John Garrick, Chairman, Advisory Committee on Nuclear Waste
Mario V. Bonaca, Chairman, Advisory Committee on Reactor Safeguards
John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
G. Paul Bollwerk, III, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Janice Dunn Lee, Director, Office of International Programs
William N. Outlaw, Director of Communications
Dennis K. Rathbun, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
Patricia G. Norry, Deputy Executive Director for Management Services, OEDO
William F. Kane, Deputy Executive Director for Homeland Protection and Preparedness, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research and State Programs, OEDO
Ellis W. Merschoff, Deputy Executive Director for Reactor Programs, OEDO
William M. Dean, Assistant for Operations, OEDO
Jacqueline E. Silber, Chief Information Officer
Michael L. Springer, Director, Office of Administration
Frank J. Congel, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Paul E. Bird, Director, Office of Human Resources
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Carl J. Paperiello, Director, Office of Nuclear Regulatory Research
Paul H. Lohaus, Director, Office of State and Tribal Programs
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV
Office of Public Affairs, Region I
Office of Public Affairs, Region II
Office of Public Affairs, Region IV

"Office of the Inspector General System Evaluation of the General License Tracking System (GLTS)"

Contract Number: GS-00F-0001N
Delivery Order Number: DR-36-03-346

September 24, 2004

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

On December 17, 2002, the President signed the E-Government Act of 2002 (Public Law 107-347), which includes the Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which include an independent evaluation of an agency's information security program and practices, and an evaluation of the effectiveness of information security control techniques. FISMA also requires an assessment of compliance with requirements and related information security policies, procedures, standards, and guidelines. As part of the Fiscal Year 2004 FISMA independent evaluation of the U.S. Nuclear Regulatory Commission's (NRC) information technology security program, Richard S. Carson Associates, Inc. (Carson Associates) reviewed security controls for the General License Tracking System (GLTS).

GLTS facilitates the tracking and accountability of general licensees and generally licensed devices with the implementation of a general license registration program. GLTS stores information about all current 10 CFR 31.5 and 31.7 general licensees, along with device information and vendor information. Of these licensees, a subset, based on a higher level of health and safety risk, will be subject to initial registration. The system includes automation necessary to facilitate mailing, receipt, and input of registrations.

PURPOSE

The system evaluation objectives were to review and evaluate the management, operational, and technical controls for GLTS.

RESULTS IN BRIEF

Carson Associates reviewed GLTS security documentation and found that GLTS security documentation is not always consistent with National Institute of Standards and Technology (NIST) guidelines, the security protection requirements are inconsistent within GLTS security documentation, and findings and recommendations resulting from testing are not consistently being tracked. None of these weaknesses are considered to be significant deficiencies or reportable conditions as defined in Office of Management and Budget guidance.

Security Documentation Is Not Always Consistent With NIST Guidelines

FISMA directs the Secretary of Commerce, on the basis of standards and guidelines developed by NIST, to prescribe standards and guidelines pertaining to Federal information systems. NIST has developed several guidelines and standards, including those for conducting risk assessments, developing security plans, and contingency plans. NRC Management Directive (MD) 12.5, *NRC Automated Information Security Program*, which was revised in September 2003, states that NRC shall comply with NIST guidance

to include guidance related to the preparation of security documentation (such as system security plans, risk assessments, and contingency plans), and other applicable NIST guidance for information technology security processes, procedures, and testing.

The previous version of MD 12.5 did not require compliance with NIST guidelines, however, Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, states that each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management. OMB periodically reminds agencies that agency security practices should be consistent with NIST guidance. The FY 2004 FISMA guidance issued by OMB specifically states that agencies must follow NIST standards and guidance. Use of NIST guidance is flexible, provided agency implementation is consistent with the principles and processes outlined within the NIST guidance.

Carson Associates reviewed the GLTS Risk Assessment, Security Plan, and Business Continuity Plan and found that while the documentation is up-to-date, it is not always consistent with NIST guidelines.

Security Protection Requirements Are Inconsistent Within Security Documentation

FISMA defines the term "information security" to mean protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Confidentiality is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Integrity is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Availability is ensuring timely and reliable access to and use of information. Confidentiality, integrity and availability are often referred to as security protection requirements or security objectives for a system. The security protection requirements defined in the GLTS Security Plan and in the FY 2003 and FY 2004 GLTS self-assessments are inconsistent.

Findings and Recommendations Resulting From Testing Are Not Consistently Being Tracked

The FY 2003 FISMA independent evaluation of NRC's information security program found that not all corrective actions resulting from security reviews and testing were being tracked and that the agency's corrective action process needed improvement. The Office of the Inspector General (OIG) recommended that the agency identify all weaknesses and recommendations from security documentation and any other security reviews, and determine in which tool the recommendations will be tracked. In November 2003, the Office of the Chief Information Officer (OCIO) issued a memo describing the agency's information technology security action item tracking process, strategy, and

tools. Carson Associates found that findings and recommendations resulting from testing of GLTS security controls and from GLTS contingency plan testing are not consistently being tracked.

RECOMMENDATIONS

This report makes five recommendations to the Executive Director for Operations to strengthen management, operational, and technical controls for GLTS. A consolidated list of recommendations can be found on page 11 of this report.

AGENCY COMMENTS

On September 13, 2004, the Executive Director for Operations provided comments concerning the draft system evaluation report. We modified the report as we determined appropriate in response to these comments.

[Page intentionally left blank]

ABBREVIATIONS AND ACRONYMS

BCP	Business Continuity Plan
CFR	Code of Federal Regulations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GLTS	General License Tracking System
ITSSTS	Information Technology Systems Security Tracking System
MD	Management Directive
NIST	National Institute of Standards and Technology
NMSS	Office of Nuclear Material Safety and Safeguards
NRC	U.S. Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SP	Special Publication

[Page intentionally left blank]

TABLE OF CONTENTS

[Page intentionally left blank]

1 Background

On December 17, 2002, the President signed the E-Government Act of 2002 (Public Law 107-347), which includes the Federal Information Security Management Act (FISMA) of 2002[1]. FISMA outlines the information security management requirements for agencies, which include an independent evaluation of an agency's information security program and practices, and an evaluation of the effectiveness of information security control techniques. FISMA also requires an assessment of compliance with requirements and related information security policies, procedures, standards, and guidelines. As part of the Fiscal Year 2004 FISMA independent evaluation of the U.S. Nuclear Regulatory Commission's (NRC) information technology security program, Richard S. Carson Associates, Inc. (Carson Associates) reviewed security controls for the General License Tracking System (GLTS).

General License Tracking System

GLTS facilitates the tracking and accountability of general licensees and generally licensed devices with the implementation of a general license registration program. GLTS stores information about all current 10 CFR 31.5 and 31.7 general licensees, along with device information and vendor information. Of these licensees, a subset, based on a higher level of health and safety risk, will be subject to initial registration. The system includes automation necessary to facilitate mailing, receipt, and input of registrations.

The NRC Office of Nuclear Material Safety and Safeguards is the GLTS system owner. The system is categorized as a Major Application[2] and is in the operational[3] phase of its life cycle.

System Evaluation Process

GLTS was evaluated by reviewing system documentation maintained by OCIO. As recommended by the Office of Management and Budget (OMB), Carson Associates reviewed the following documents for adherence to standards and consistency with guidelines issued by the National Institute of Standards and Technology (NIST).

- GLTS Risk Assessment, July 2002
- GLTS Security Plan, August 2002
- GLTS Business Continuity Plan, March 2004
- GLTS Security Test and Evaluation Report, August 2002
- GLTS System Certification Report, September 2002
- Certification and Accreditation Statement, September/October 2002

[1] The Federal Information Security Management Act of 2002 was enacted on December 17, 2002, as part of the E-Government Act of 2002 (Public Law 107-347), and replaces the Government Information Security Reform Act, which expired in November 2002.

[2] An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

[3] A system's life cycle typically comprises five phases: initiation, development/acquisition, implementation, operation/maintenance, and disposal. In the operation/maintenance phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced.

- Privacy Impact Assessment
- FY 2003 and draft FY 2004 GLTS Self-Assessment

The documents were reviewed to determine whether they are consistent with NIST guidance and whether they describe the management[4], operational[5], and technical[6] controls in place for GLTS.

2 Purpose

The system evaluation objectives were to review and evaluate the management, operational, and technical controls for GLTS.

3 Findings

Carson Associates reviewed GLTS security documentation and found that:

- GLTS security documentation is not always consistent with National Institute of Standards and Technology guidelines.
- Security protection requirements are inconsistent within GLTS security documentation.
- Findings and recommendations resulting from testing are not consistently being tracked.

None of these weaknesses are considered to be significant deficiencies or reportable conditions as defined in Office of Management and Budget guidance.

3.1 Security Documentation Is Not Always Consistent With NIST Guidelines

FISMA directs the Secretary of Commerce, on the basis of standards and guidelines developed by NIST, to prescribe standards and guidelines pertaining to Federal information systems. NIST has developed several guidelines and standards, including those for conducting risk assessments, developing security plans, and contingency plans. NRC Management Directive (MD) 12.5, *NRC Automated Information Security Program*, which was revised in September 2003, states that NRC shall comply with NIST guidance to include guidance related to the preparation of security documentation (such as system security plans, risk assessments, and contingency plans), and other applicable NIST guidance for information technology security processes, procedures, and testing.

The previous version of MD 12.5 did not require compliance with NIST guidelines, however, OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, states that each agency's program shall implement

[4] The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
[5] The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
[6] The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce[7], the General Services Administration and the Office of Personnel Management. OMB periodically reminds agencies that agency security practices should be consistent with NIST guidance. The FY 2004 FISMA guidance issued by OMB[8] specifically states that agencies must follow NIST standards and guidance. Use of NIST guidance is flexible, provided agency implementation is consistent with the principles and processes outlined within the NIST guidance.

Carson Associates reviewed the GLTS Risk Assessment, Security Plan, and Business Continuity Plan and found that while the documentation is up-to-date, it is not always consistent with NIST guidelines.

GLTS Security Plan Does Not Describe All Security Controls Identified As In-Place

OMB A-130 states that security plans shall be consistent with guidance issued by NIST. NIST Special Publication (SP) 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that the purpose of a security plan is to provide an overview of the security requirements of the system and describe controls in place or planned for meeting those requirements. NIST SP 800-18 also states that the security plan should fully identify and describe the controls currently in place, or planned for the system. However, Carson Associates found several areas in the Final System Security Plan for GLTS, dated August 23, 2002, where controls were not described.

In order to identify what controls are currently in place for GLTS, Carson Associates reviewed and analyzed two other documents in conjunction with the GLTS Security Plan – the GLTS self-assessment, and results from security test and evaluation of GLTS controls conducted during the certification and accreditation of GLTS.

FISMA requires agencies to test the management, operational, and technical controls of every information system identified in their inventory no less than annually. OMB has instructed agencies to use NIST SP 800-26, *Self-Assessment Guide for Information Technology Systems*, to conduct the annual reviews. NIST SP 800-26 is based on the Chief Information Officer Council's "Federal Information Technology Security Assessment Framework" (the Framework). The Framework comprises five levels to guide agency assessments of their security programs and assist in prioritizing efforts for improvement. Level 1 reflects that an asset has documented security policy. At Level 2, the asset also has documented procedures and controls to implement the policy. For Level 3, procedures and controls have been implemented to protect the asset. Level 4 indicates that procedures and controls are tested and reviewed. Finally, at Level 5, the asset has procedures and controls fully integrated into a comprehensive program.

Carson Associates reviewed the FY 2003 GLTS self-assessment in order to identify controls in place for GLTS. Any controls marked at least at a Level 3 in the GLTS self-assessment are

[7] NIST is part of the Technology Administration within the Department of Commerce.
[8] OMB Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act, dated August 23, 2004.

considered to be in place based on the above definitions. The FY 2003 self-assessment was reviewed as the agency had only provided a draft of the FY 2004 self-assessment when the fieldwork was conducted.

Carson Associates also reviewed the results of the security test and evaluation of GLTS controls conducted during the certification and accreditation of GLTS. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Appendix D of the GLTS Security Test and Evaluation Report, dated August 16, 2002, includes test procedure worksheets used to record the results of the testing. The test objectives on the test procedure worksheets correspond to the control objectives in the NIST SP 800-26 self-assessment. Each test objective is marked as either pass, fail, or not applicable. A test objective marked as pass represents a security control that is in place.

As a result of the review of the GLTS Security Plan, self-assessment, and security test and evaluation results, Carson Associates identified several cases where the information in the GLTS Security Plan, self-assessment and test procedure worksheets is inconsistent. The following are some examples:

- Controls for matching personnel files with user accounts to ensure that terminated or transferred individuals do not retain system access are marked as "pass" on the test procedure worksheets, however the same control is marked as "not applicable" in the FY 2003 GLTS self-assessment. In the FY 2004 GLTS self-assessment, the control is marked to indicate the control is done at the local area network level, not at the application level. The GLTS Security Plan does not describe these controls.
- The test control worksheets indicate that penetration testing is performed on the system. The GLTS self-assessment indicates that penetration testing is the responsibility of the local area network/wide area network and/or Data Center. Penetration testing is not described in the GLTS Security Plan.
- ***OFFICIAL USE ONLY BULLET REDACTED***

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Update the GLTS Security Plan to describe all controls currently in place. In-place controls are those marked at least at Level 3 in the self-assessment, and that were

documented as passed in the last Security Test and Evaluation Report, or in any test and evaluation on controls added since publication of that report.

2. Update the GLTS self-assessment to reflect controls in place. In-place controls are those that were documented as passed in the last Security Test and Evaluation Report, or in any test and evaluation on controls added since publication of that report.

GLTS Business Continuity Plan Is Not Consistent With NIST Guidelines

Carson Associates reviewed the GLTS Business Continuity Plan (BCP), dated March 31, 2004. Guidance on developing contingency plans can be found in NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, which was published in June 2002. As recommended by OMB, Carson Associates reviewed the GLTS BCP for consistency with NIST guidelines and found that in some instances, the GLTS BCP is not consistent with NIST guidelines.

According to the agency, NRC requires annual updates of all BCPs, however NRC only requires conformance with current NIST guidance at the time of re-accreditation. This policy is not documented in any agency management directive or in any documentation reviewed by Carson Associates. Carson Associates was informed of this policy during the exit conference held to discuss the findings of the GLTS system evaluation. Subsequent to the exit conference, Carson Associates reviewed previous NIST guidance on the preparation of contingency plans, Federal Information Processing Standards (FIPS) Publication 87, *Guidelines for ADP Contingency Planning*, and found that the GLTS BCP (both the 2004 version and the previous version, dated September 27, 2002) is also not consistent with the FIPS 87 guidance. It should be noted that the previous version of the GLTS BCP was published in September 27, 2002, which was after NIST issued SP 800-34. As stated earlier in this report, while the version of MD 12.5 that was in effect at the time the GLTS BCP was published did not require compliance with NIST guidelines, OMB requires agencies to follow NIST standards and guidance.

NIST SP 800-34 states that the contingency plan should be a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to the plan should be recorded in a record of changes. The GLTS BCP does not include any information on what changes have been made to the plan and when. Without this information, Carson Associates could not determine whether the BCP was updated as part of the annual requirement, or as part of a system re-accreditation. The only indication that the BCP was a revision was the word "Revised" on the cover page. FIPS 87 also states that an essential element of any volatile document, such as a contingency plan, is a method of recording changes to the document.

NIST SP 800-34 describes notification procedures and states that they should be documented in the plan for both events that occur with and without prior notice. For example, advanced notice is often given that a hurricane will affect an area or that a computer virus is expected on a certain date. However, there may be no notice of equipment failure or a criminal act. The procedures should describe the methods used to notify recovery personnel during business and non-business hours. Prompt notification is important for reducing the effects on the system; in some cases, it

may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash.

NIST SP 800-34 also states that personnel to be notified in the event of a disaster should be clearly identified in the contact list appended to the plan. The list should identify personnel by their team position, name, and contact information (e.g., home number, work number, pager number, e-mail addresses, and home addresses). FIPS 87 also stresses the importance of including the name, address, and phone numbers of all people who may be required in any backup or recovery scenario in the BCP.

OFFICIAL USE ONLY PARAGRAPH REDACTED

NIST SP 800-34 defines the reconstitution phase as when recovery activities are terminated and normal operations are transferred back to the organization's facility. The reconstitution phase should specify teams responsible for restoring or replacing both the site and the system. The GLTS BCP does not include procedures for restoring system operations that include procedures for cleaning the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. While FIPS 87 does not discuss specific procedures to be followed for cleaning the alternate site of any equipment or other materials belonging to the organization, these procedures are necessary to ensure that no sensitive materials remain at the alternate site.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

3. Update the GLTS Business Continuity Plan to include the following changes:

   - Record modifications to the plan in a record of changes to include what changes were made (e.g., the page numbers or section numbers where the changes were made), why the changes were made (e.g., annual update or update during re-accreditation), and date of change.
   - Describe the methods used to notify recovery personnel during business and non-business hours.

- Incorporate all teams roles and responsibilities and relevant points of contact information for team leaders, alternate team leaders, and team members.
- Include procedures for restoring system operations, with a focus on how to clean the alternate site of any equipment or other materials belonging to the organization.

3.2 Security Protection Requirements Are Inconsistent Within Security Documentation

FISMA defines the term "information security" to mean protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Confidentiality is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Integrity is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Availability is ensuring timely and reliable access to and use of information. Confidentiality, integrity and availability are often referred to as security protection requirements or security objectives for a system.

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires all Federal agencies to categorize their systems by assigning potential impact levels to the three security objectives. The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.[9] The potential impact is moderate (medium) if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. The potential impact is high if 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.

The GLTS Security Plan defines protection requirements for GLTS as follows:

- Confidentiality – Medium
- Integrity – High
- Availability – Medium

However, the FY 2003 GLTS self-assessment and FY 2004 draft GLTS self-assessment define protection requirements for GLTS as follows:

- Confidentiality – Medium
- Integrity – High
- Availability – Low

[9] Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

The protection requirements should be consistent across the security documentation for a system. A change in protection requirements could indicate a need to re-evaluate the risks to the systems, especially if the change is from a lower rating to a higher one. If the protection requirements have changed since the GLTS Security Plan was finalized, then an explanation for the change should be noted on the GLTS self-assessment.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

4. Update the GLTS Security Plan and/or GLTS self-assessment to consistently define the protection requirements (confidentiality, integrity, availability).

3.3 Findings and Recommendations Resulting From Testing Are Not Consistently Being Tracked

The FY 2003 FISMA independent evaluation of NRC's information security program found that the agency's corrective action process needed improvement. NRC has two primary tools for tracking the progress of corrective actions related to correcting weaknesses identified during the annual agency security review, the OIG independent evaluation, various security documents, and other security studies conducted by or on behalf of the agency. At a high level, NRC uses the POA&M submitted to OMB to track corrective actions from the OIG annual independent evaluation, and the agency's annual review. At a more detailed, level, NRC uses the NRC Information Technology Systems Security Tracking System (ITSSTS) to track the progress of internal corrective actions (i.e., those not reported to OMB). ITSSTS is used to track more specific corrective actions, such as those resulting from risk assessments; security test and evaluation associated with the certification and accreditation process; and contingency plan testing.

The FY 2003 FISMA independent evaluation of NRC's information security program also found that not all corrective actions resulting from security reviews and testing were being tracked. The OIG recommended that the agency identify all weaknesses and recommendations from security documentation and any other security reviews, and determine in which tool the recommendations will be tracked. In November 2003, OCIO issued a memo describing the agency's information technology security action item tracking process, strategy, and tools. The memo describes the types of activities that might identify security weaknesses in NRC information technology systems and describes the two tools used by NRC for tracking the process of security corrective actions – the FISMA POA&M and the ITSSTS. Carson Associates found that findings and recommendations resulting from testing of GLTS security controls and from GLTS contingency plan testing are not consistently being tracked.

Not All Findings Resulting from the GLTS Certification and Accreditation Are Being Tracked

The GLTS Risk Assessment identified eight risks and Carson Associates found that all of them were tracked in the ITSSTS. The GLTS Security Test and Evaluation Report also identified eight risks, however these were not the same eight risks identified in the GLTS Risk Assessment.

Two of risks identified in the GLTS Risk Assessment were not identified during the security test and evaluation. These risks were 1) no individual assigned security responsibility for GLTS, and 2) no documented termination procedures are in place to ensure user access to GLTS is removed. These risks are being tracked in the ITSSTS. However, two new risks were identified during the security test and evaluation. These risks were 1) no system security plan in place for GLTS, and 2) adequate audit trails are not maintained by GLTS. However, these two risks are not being tracked in the ITSSTS.

Carson Associates could not determine why the two new risks identified during security test and evaluation were not being tracked in the ITSSTS. A possible cause is that since the total number of risks identified during the risk assessment and the security test and evaluation were the same, the two new risks may have been overlooked.

Findings and Recommendations Resulting from the GLTS BCP Testing Are Not Consistently Being Tracked

Carson Associates reviewed the GLTS Business Continuity Test Report, dated May 18, 2004. Tests of the BCP were conducted in April 2004 by using a walk through tabletop exercise. Three tests scenarios were performed to include: (1) GLTS server outage, (2) Two White Flint North Data Center is unavailable, and (3) Loss of availability of both NRC Buildings (One and Two White Flint North). The testing identified four shortcomings, and resulted in three recommendations. The agency is tracking the four shortcomings in their internal tracking system, but is tracking the three recommendations in the POA&M to OMB.

OFFICIAL USE ONLY PARAGRAPH REDACTED

OFFICIAL USE ONLY PARAGRAPH REDACTED

There is no recommendation that correlates to the 1st shortcoming, and the last recommendation does not correlate to any of the shortcomings. All four shortcomings are being tracked in the ITSSTS, and all three recommendations are being tracked in the POA&M submitted to OMB. However, since there is not a relationship between all of the shortcomings and the recommendations, the shortcomings and recommendations are not being tracked consistently across the agency's tracking systems. The first shortcoming is only being tracked in the ITSSTS, and the last recommendation is only being tracked in the POA&M submitted to OMB. Tracking shortcomings (i.e., weaknesses) in one system and recommendations in another could result in weaknesses not being addressed or overlooked, or in recommendations not being corrected on time.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

5. Track all actions items resulting from testing of the GLTS security controls and contingency plan in either the agency's internal tracking system or in the agency's plan of action and milestones submitted to OMB.

4 Consolidated List of Recommendations

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Update the GLTS Security Plan to describe all controls currently in place. In-place controls are those marked at least at Level 3 in the self-assessment, and that were documented as passed in the last Security Test and Evaluation Report, or in any test and evaluation on controls added since publication of that report.

2. Update the GLTS self-assessment to reflect controls in place. In-place controls are those that were documented as passed in the last Security Test and Evaluation Report, or in any test and evaluation on controls added since publication of that report.

3. Update the GLTS Business Continuity Plan to include the following changes:

   - Record modifications to the plan in a record of changes to include what changes were made (e.g., the page numbers or section numbers where the changes were made), why the changes were made (e.g., annual update or update during re-accreditation), and date of change.
   - Describe the methods used to notify recovery personnel during business and non-business hours.
   - Incorporate all teams roles and responsibilities and relevant points of contact information for team leaders, alternate team leaders, and team members.
   - Include procedures for restoring system operations, with a focus on how to clean the alternate site of any equipment or other materials belonging to the organization.

4. Update the GLTS Security Plan and/or GLTS self-assessment to consistently define the protection requirements (confidentiality, integrity, availability).

5. Track all actions items resulting from testing of the GLTS security controls and contingency plan in either the agency's internal tracking system or in the agency's plan of action and milestones.

5 OIG Response to Agency Comments

On September 13, 2004, the Executive Director for Operations provided comments concerning the draft system evaluation report. We modified the report as we determined appropriate in response to these comments.

SCOPE AND METHODOLOGY

To perform the GLTS system evaluation, Carson Associates reviewed the system's security documentation, including the Security Plan, Risk Assessment, self-assessment, Business Continuity Plan, System Test and Evaluation Report, Certification and Accreditation documentation, and the completion of weaknesses addressed, if any, within the FY 2003 plan of action and milestones. Comprehensive document checklists were used in the evaluation process.

The work was conducted from June 2004 to August 2004 in accordance with guidelines from the National Institute of Standards and Technology, and best practices for evaluating security controls. Diane Reilly and Jane Laroussi from Carson Associates conducted the work.

[Page intentionally left blank]