

**Security Testing and Certification of the
Modernized Infrastructure Needs to Be
Strengthened**

June 2003

Reference Number: 2003-20-127

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

June 27, 2003

MEMORANDUM FOR ACTING DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Assistant Inspector General for Audit (Small Business and
Corporate Programs)

SUBJECT: Final Audit Report - Security Testing and Certification of the
Modernized Infrastructure Needs to Be Strengthened
(Audit # 200320036)

This report presents the results of our review of the security testing, certification, and accreditation of the Internal Revenue Service's (IRS) modernized infrastructure. The overall objective of this review was to determine the adequacy and effectiveness of security testing performed on the first release of the Security and Technology Infrastructure Release (STIR) project. We performed an evaluation of the Certification Program Office's certification and accreditation¹ procedures, which include the security testing and evaluation processes. We also performed a detailed assessment of the STIR project's security test plans and respective test results, including reviews of evaluation reports.

In summary, the STIR project provides a secure technical infrastructure² to support and enable the delivery of the IRS' modernized business systems. For the IRS' Business Systems Modernization Office (BSMO) and the PRIME contractor,³ the STIR is the first Business Systems Modernization project to undergo the security certification testing and

¹ Certification requires a comprehensive evaluation of technical and nontechnical security features to determine the extent to which system design and implementation meet a specified set of security requirements. Accreditation is an official declaration by the responsible official (i.e., system owner) that an information system or network is approved to operate with prescribed security safeguards.

² Infrastructure refers to the hardware, software, and security systems that computer systems use to communicate and share information.

³ The PRIME contractor is the Computer Sciences Corporation, which heads an alliance of leading technology companies assisting the IRS with modernizing its computer systems and related technology.

accreditation processes as required by the Office of Management and Budget and the Department of the Treasury.⁴ Many challenges were encountered during this process, but the completion of the STIR in May 2002 was a monumental step in providing opportunities for the development and deployment of all other modernized projects. The growth of the BSMO and cooperation among various IRS organizations and management has contributed to the success of the first release of the STIR.

However, the IRS did not:

- Fully and accurately complete its security testing.
- Finalize the formal certification.
- Provide system accreditation before deploying the STIR.

These incomplete processes could leave the system exposed to potential threats and vulnerabilities from unauthorized persons gaining access to taxpayer data. There are several critical areas where improvement is needed to ensure that management, testing, certification, and accreditation processes are adequately performed.

First, the IRS authorized the STIR project to process sensitive taxpayer information without having complete formal documentation of the results of security testing. As a result, the initial certification memorandum for the project had to be reissued 5 months later, stating that the unconditional certification would be changed to a conditional certification if key risks were not addressed in the next release of the STIR. System accreditation also did not occur until 5 months after the system was put into production. Results of security testing are a key input to the security certification and accreditation process.

In addition, limitations in the security testing and reporting of test findings increased the risks to the deployed STIR. For example, testing was not performed on all production components, it was executed concurrently with other tests to alleviate escalating schedule delays, and testing results were not always accurately reported.

Lastly, documentation detailing an accurate description of the STIR's physical design and components was not timely provided for the Certification Program Office to use in planning and executing the security testing. As a result, the testers were not able to execute all originally planned security test cases detailed in the security test plan.

We recommended that the Acting Deputy Commissioner for Modernization & Chief Information Officer require a complete formal security certification and accreditation package prior to approving the processing of sensitive data for all future Business Systems Modernization projects. We also recommended that the security risks associated with future system deployments be reduced by ensuring that security tests are performed on all physical components of the STIR located at every functional site.

⁴ The Office of Management and Budget (Circular A-130) and the Department of the Treasury (Security Manual TD P-71-10) require all information systems that process sensitive but unclassified information (e.g., taxpayer data) to be certified and accredited for operation.

The PRIME contractor should be informed that security tests should not be executed concurrently with other critical test phases. The Certification Program Office should develop improved processes to ensure that all security testing results are accurately and completely disclosed. Documentation listing all failed or inaccurately disclosed test cases from the first release of the STIR's security testing report should be prepared and attached to the security test report for the certification and accreditation of the next STIR release. If the IRS decides, for business reasons, to continue with any of these practices for other systems, these actions and their associated risks should be clearly communicated within the security test report that is part of the certification package.

Lastly, we recommended that the Infrastructure Project Office and the PRIME contractor be required to produce updated and accurate copies of the critical STIR documentation for use in future system security monitoring, as well as for use by the Information Technology Services organization in maintaining the system. In the future, accurate and complete system documentation should be required from the contractor prior to beginning security testing. Additionally, any deviations from the security test plan should be clearly explained in the security test report.

Management's Response: The Acting Deputy Commissioner for Modernization & Chief Information Officer responded that he concurred with report observations about the need to provide timely and formal documentation during the security certification testing and accreditation processes. He also responded that the IRS is continuing actions to strengthen its security certification capabilities and that processes will be improved.

However, the Acting Deputy Commissioner for Modernization & Chief Information Officer disagreed with three of the conditions included in our report. First, he did not concur with the finding that the certification and accreditation processes for the STIR were not completed until several months after the project became operational. He stated that the Deputy Commissioner for Modernization & Chief Information Officer issued an interim certification memorandum on the same day the STIR project was deployed.

Second, the Acting Deputy Commissioner for Modernization & Chief Information Officer disagreed that security testing was limited, concurrent, or that test results were inaccurately reported. He stated that the Certification Program Office conducted an independent security test to verify and validate the STIR project's security functionality against IRS security requirements.

Third, the Acting Deputy Commissioner for Modernization & Chief Information Officer stated that the IRS did not allow risky concurrent testing as the report indicates. While security testing was conducted on the same day as other tests, they were not conducted at the same times.

Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment: We believe the conditions reflected in this report are factual and relevant, and the following comments further support our position. Regarding the issue of the certification of the STIR project, we agree that an interim certification was issued on the day the STIR project was deployed. However, our concern is that not all

of the relevant information on which to base a decision to certify a system was available at that time. As detailed in our report, the PRIME contractor had not completed or provided the Security Evaluation Report and Certification Statement. This information was not provided to the IRS until over a month after the STIR project was deployed. The exception we are taking to the STIR certification process is that the interim certification was issued before all final testing results and evaluations were presented to the IRS. We agree with the IRS' Enterprise Life Cycle requirements that a certification package must be completed prior to a system processing live data, and this package must include a report of the results of the security testing. Results of security testing are one of the most critical components of a system certification, especially in a system as critical as the security infrastructure. However, in this case the IRS had not followed its own procedures.

As to the issue of the IRS security testing being limited, performed concurrently, or inaccurately reported, we still maintain that the processes and methods followed by the IRS limited the effectiveness of the security tests. The Acting Deputy Commissioner for Modernization & Chief Information Officer indicated that limited security testing was performed because the IRS employed a testing methodology called "Type" accreditation from the National Institute of Standards and Technology (NIST) guidelines to justify testing only one of the two Registered User Portal sites. We maintain that using Type accreditation for a system as critical as the infrastructure is inappropriate, and we provide further detail on this issue in the body of the report. We also believe that, while it was inappropriate to apply Type accreditation to the STIR, the IRS relied upon the advantages of that guidance without following or performing the recommended or suggested NIST processes and procedures that should occur to provide the necessary support for a Type accreditation.

The Acting Deputy Commissioner for Modernization & Chief Information Officer further responded that the IRS did not allow risky concurrent testing because IRS processes provide for system test phases to occur on the same day but at different times of the day. We believe that each test phase, whether it is integration, deployment site readiness, or security testing, should occur independently and be completed prior to starting another test phase. This is beneficial because changes are often made to systems based on test results, so all tests should be completed and changes made before a system is submitted for security testing to ensure the final configuration is tested. We also believe that it is a risky practice to perform multiple testing phases on the same system or components on the same day, especially when each test phase can require several weeks to complete. In the case of the STIR testing, tests had to be re-performed and the certification process repeated several times to ensure security requirements were still in compliance after changes to the system were made.

We recognize the applications currently running on the STIR are considered lower-risk by the IRS and currently contain only minimal amounts of accessible taxpayer data. Still, we believe it is critical that the IRS use these lower-risk applications to develop and improve the security testing processes that will be needed to successfully deploy more complex and significant applications in the future. While we disagree with some of the responses provided by the Acting Deputy Commissioner for Modernization & Chief

Information Officer, we do not intend to elevate our disagreement to the Department of the Treasury for resolution.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions, or Margaret E. Begg, Acting Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Table of Contents

Background	Page 1
The First Release of the Modernized Infrastructure Was Deployed in 2002.....	Page 2
Certification and Accreditation Processes Were Not Completed Until Several Months After Project Deployment.....	Page 3
<u>Recommendation 1</u> :	Page 5
<u>Recommendation 2</u> :	Page 6
Limitations of Security Testing and Inaccurate Reporting of Results Could Increase Project Risks.....	Page 6
<u>Recommendation 3</u> :	Page 11
<u>Recommendation 4</u> :	Page 12
<u>Recommendation 5</u> :	Page 13
Critical Infrastructure Documentation Was Not Provided Timely	Page 14
<u>Recommendations 6 and 7</u> :	Page 16
<u>Recommendation 8</u> :	Page 17
Appendix I – Detailed Objective, Scope, and Methodology	Page 18
Appendix II – Major Contributors to This Report.....	Page 19
Appendix III – Report Distribution List	Page 20
Appendix IV – Management’s Response to the Draft Report	Page 21

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Background

The Security and Technology Infrastructure Release (STIR) project provides a secure technical infrastructure¹ to support and enable the delivery of the Internal Revenue Service's (IRS) modernized business systems. The STIR consists of numerous hardware, software, and security system components installed at different geographical locations, which are integrated together to serve as the central backbone for all other modernized computer systems. The STIR project is designed to provide a fully secure computing environment based upon web technology, which uses the Internet as a primary means for communicating and delivering taxpayer information.

The Internet is an increasingly important tool for information and commerce within the United States. However, there are inherently high security and privacy risks when combining the use of Internet technology with a business systems environment. During the creation of the STIR, the Business Systems Modernization Office (BSMO) and the PRIME contractor² were challenged with ensuring that a secure environment existed to safely store and transport taxpayer data.

There are several guidelines and principles that the BSMO and the PRIME contractor should adhere to when developing security for an information system. However, the most critical information system security process that all Federal Government agencies must undergo is security certification and accreditation.³ The main purpose of system certification and accreditation is to provide documented evidence (security test cases and results) that the system meets security standards and that system owners accept the

¹ Infrastructure refers to the hardware, software, and security systems that computer systems use to communicate and share information.

² The PRIME contractor is the Computer Sciences Corporation, which heads an alliance of leading technology companies assisting the IRS with modernizing its computer systems and related technology.

³ Certification requires a comprehensive evaluation of technical and nontechnical security features to determine the extent to which system design and implementation meet a specified set of security requirements. Accreditation is an official declaration by the responsible official (i.e., system owner) that an information system or network is approved to operate with prescribed security safeguards.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

security risks related to its operation. This provides an assurance that the BSMO and the PRIME contractor have performed all the necessary steps to adequately safeguard the confidentiality and integrity of taxpayer data. The IRS' Certification Program Office (CPO) and its subcontractors perform the security testing of modernized systems and recommend for or against certification and accreditation.

The audit was conducted in the BSMO facilities in New Carrollton, Maryland, between August 2002 and February 2003 in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

The First Release of the Modernized Infrastructure Was Deployed in 2002

In May 2002, the first release of the STIR was completed and began processing taxpayer requests for refund information via the Internet. This was a monumental step in providing opportunities for the development and deployment of all other modernized projects. For the BSMO and the PRIME contractor, the STIR was the first Business Systems Modernization (BSM) project to undergo detailed security certification testing and accreditation processes.

With critical schedule delays and budgetary constraints, the STIR project team and the IRS' Office of Security Services faced many challenges during the design, development, and testing of the security features of the STIR project. One of these major challenges was ensuring the coordination and cooperation to provide the required independent security reviews. For example, the Office of Security Services and its subordinate offices provided specialized expertise to ensure that all security requirements were complete.

Due to the nature of modernized systems, the security requirements for modernized projects are more robust than ever before. As a result, the various IRS offices must continue to work together to ensure successful development and deployment of other modernized projects. The cooperation between the IRS' security offices and the BSMO contributed to the deployment of the first release of the STIR.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

While the STIR was deployed and has been supporting other BSM applications, the IRS did not fully and accurately complete the security testing, certification, and accreditation processes, which could leave the STIR system exposed to potential threats and vulnerabilities from unauthorized persons gaining access to taxpayer data. We recognize the applications currently running on the STIR are considered lower-risk by the IRS and currently contain only minimal amounts of accessible taxpayer data. Still, we believe it is critical that the IRS use these lower-risk applications to develop and improve the security testing processes that will be needed to successfully deploy more complex and significant applications in the future. We identified the following critical areas where improvement is needed to ensure that management, testing, certification, and accreditation processes are adequately performed.

Certification and Accreditation Processes Were Not Completed Until Several Months After Project Deployment

The accreditation for the STIR was not completed until 5 months after the system became operational in May 2002. Although an interim certification had been granted, a key element of the certification package,⁴ the formal report of the results of security testing, was not completed until over a month after the project was authorized to begin processing sensitive taxpayer data. The interim certification was revised and reissued in October 2002, stating that the unconditional certification would be changed to a conditional certification if key risks were not addressed in the next release of the STIR. The accreditation letter was not signed and issued until later in October 2002, after the revised certification was issued.

The Office of Management and Budget Circular A-130 (*Management of Federal Information Resources*, dated February 1996), and the Department of the Treasury Security Manual (Treasury Directive TD P-71-10, dated August 1999), require all information systems that process sensitive but unclassified information (e.g., taxpayer data) to be certified and accredited for operation. Additionally, the

⁴ A Security Certification Package includes detailed reports providing the configurations, settings, components, diagrams, management, risks, and security testing results of computer systems.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Enterprise Life Cycle (ELC)⁵ requires that the certification package be completed prior to a system processing live data, and this package must include a report of the results of the security testing. Results of security testing are one of the most critical components of a system certification.

Although the last security testing was carried out in April 2002, the formal report documenting the results of the tests was not completed until June 2002. The certification package is used to support the authorization and accreditation of a system, which includes the formal review and issuance of official declarations.

When we discussed this issue with officials from the Office of Management Assurance and the BSMO, they indicated that the executives that met to discuss the risks of processing sensitive taxpayer data were aware of the results of the security testing. The officials also indicated that the certification that had been granted was sufficient, but agreed that the formal accreditation did not come until several months later.

Additionally, the security and BSMO officials indicated that the guidance addressing security and privacy requirements prior to authorizing processing of sensitive data was inaccurately stated in the ELC. This guidance indicated that security documents must be completed prior to moving out of the development phase. Although we are not convinced that the ELC is inaccurate in this area, if the processes as defined are not being followed, this needs to be documented. Additionally, if changes are needed, these should be made quickly so that other projects will not attempt to follow the inaccurate processes.

While we understand that time is often critical at the deployment phase of a project, security certification and accreditation is very important and should be fully addressed prior to authorizing a system to process sensitive data, especially a system as critical as the security infrastructure of the modernized environment. Granting

⁵ The ELC provides detailed guidance and methodology to be followed during the planning, design, development, and deployment stages of the IRS' modernized projects.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

interim certification for a system as critical as the STIR without having all the security test results formally reported could allow both security risks to not be adequately addressed and potential threats of unauthorized access to taxpayer data to exist on systems it supports.

Recommendations

To ensure that future BSM projects meet security requirements and IRS officials clearly understand the risks related to the projects and the impacts on their operations, we recommend that the Acting Deputy Commissioner for Modernization & Chief Information Officer:

1. Ensure that security certification and accreditation is performed, with all formal documents completed and approved, prior to allowing any future BSM project to process sensitive taxpayer data.

Management's Response: The Acting Deputy Commissioner for Modernization & Chief Information Officer responded that the IRS certification and accreditation process allows for an informed management decision to be made on a project-by-project basis that considers the project risks at the completion of the security test and evaluation. He further stated that if there is an immediate business need and risks are moderate to low, IRS management may proceed to authorize processing. Accreditation paperwork will follow as soon as possible. The response also stated that the improved certification and accreditation within the ELC process will indicate what document is needed that communicates this authority.

Office of Audit Comment: Specific guidance already exists within the ELC and the Department of the Treasury Security Manual TD P-71-10 that allows for a system to temporarily operate without full compliance to certification and accreditation. While we do not recommend this scenario, if this situation does occur, a written exception must be obtained from the IRS Office of Security, Privacy, and Oversight. This process was not followed during the certification and accreditation for the STIR. Our concern is that not all of the relevant information on which to base a

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

decision to certify a system was available at that time. As detailed above, the PRIME contractor had not completed or provided the Security Evaluation Report and Certification Statement. This information was not provided to the IRS until over a month after the STIR project was deployed. The exception we are taking to the STIR certification process is that the interim certification was issued before all final testing results and evaluations were presented to the IRS. We continue to maintain that all security certifications and accreditations should be performed, and all formal documents completed and approved, prior to allowing the system processing of taxpayer information as stated in the ELC. Results of security testing are one of the most critical components of a system certification, especially in a system as critical as the security infrastructure.

2. Review the ELC to determine if the guidance related to security requirements prior to authorizing deployment of a system is accurate. If not, request immediate changes to the ELC to ensure future projects are following correct guidance.

Management's Response: The Acting Deputy Commissioner for Modernization & Chief Information Officer responded that the Security Test and Evaluation must occur in the deployed environment following the Deployment Site Readiness Test. The response also stated that the test, and the resulting Security Evaluation Report, cannot be addressed in the developmental phase (milestone 4 of the ELC), but instead must be completed in the deployment phase (milestone 5). He also stated that corrective actions are underway to enhance the documentation, the timing related to milestones, and the timing of security tests within the ELC process.

Limitations of Security Testing and Inaccurate Reporting of Results Could Increase Project Risks

Security testing is one of the final steps prior to making the decision to put a system into production to process live data. Because of the timing of this testing, it is tempting for the business project team to try to make up for any schedule slippages that occur during any of the prior development steps by limiting this testing, testing concurrently with other system tests, or rushing through the documentation of the test results. Each of these approaches can increase the level

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

of risk in the production system because of a decrease in focus on the critical security testing. Risks include unauthorized access to taxpayer data, as well as potential system attacks by hackers.

Security testing of the STIR's physical components was limited

The security testing for the STIR did not include reviews of all components (hardware and software) within the infrastructure. Specifically, there are two locations where the Registered User Portals (RUP)⁶ reside. Both locations contain two identical sets of physical components. However, only one set of physical components at the first RUP location was tested, while the remaining set in the same location, as well as the two sets in the other location, were not tested as part of the security testing process.

Management in the CPO indicated that they were justified in not testing all the STIR's physical components because they were following a process known as a "Type" accreditation, which is described in guidelines issued by the National Institute of Standards and Technology (NIST).⁷ A Type accreditation can be used when the same system or configuration is being installed in multiple locations.

However, this Type accreditation should not have been used for a project with such strategic importance to the IRS' modernization program, nor was it executed properly for the STIR deployment, as follows:

- The most critical reason a Type accreditation was inappropriate is because the STIR components are key elements protecting the modernized systems against attacks and vulnerabilities. If all the STIR components did not undergo security testing, undetected weaknesses and openings may exist for malicious attackers to obtain sensitive taxpayer information.

⁶ A RUP is a doorway for users on the Internet to obtain access into the STIR's computing network.

⁷ *Guidelines for the Security Certification and Accreditation of Federal Information Systems* (NIST Special Publication 800-37).

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

- A Type accreditation is typically used when deploying a system at multiple site locations when site testing would be cost-prohibitive. The RUP functionality was deployed at only two locations.
- A Type accreditation requires that developmental security testing be performed prior to deploying the system in multiple locations, and then performing operational security testing at each location where the system is deployed. These steps were not performed during the STIR's security testing.
- According to NIST guidelines, a Type accreditation is a form of interim (temporary) accreditation for systems that do not currently meet the security requirements as stated in the security plan and for which all of the necessary controls are not implemented and operating effectively. When an interim accreditation is provided, a statement of the risk associated with that method of accreditation must be completed along with documentation that clearly defines the intended operating environment and associated constraints in which this system must operate. This was not done for the STIR.
- In reviewing the results from another phase of the STIR's testing, we found two tests that were conducted at both RUP sites that passed at one location but failed at the other location. This indicates that the STIR configurations were not exact duplications at each location, even though they were supposed to be exactly the same implementation. In addition, penetration testing recently conducted at one of the RUP locations as part of testing the second release of the STIR identified four high-risk findings at that site. We believe these findings may leave the initial release of the STIR vulnerable, as well, and possibly could have been addressed if security testing had initially been performed at both locations.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Risky concurrent testing in different testing environments was allowed

The first release of the STIR was experiencing schedule delays when it came time to execute the three most critical phases of project testing: integration testing,⁸ security testing, and site readiness testing.⁹ To alleviate further schedule delays, all three critical testing phases were performed concurrently, and the security testing processes were shortened. The testing was performed during the following dates:

- Integration Testing - February 5 to April 23, 2002.
- Site Readiness Testing - February 11 to April 26, 2002.
- Security Testing - March 25 to April 25, 2002.

The integration testing of the STIR occurred within a controlled testing environment. During this time, the STIR was still undergoing design and configuration changes, which would require modification to software and hardware components. In addition, to address failures during security or site readiness testing, changes were made. If the security tests were executed and system modifications resulting from failures in site readiness or integration testing occurred at the same time, it would potentially negate the results of any security tests performed.

The amount of configuration management¹⁰ and regression testing¹¹ required when testing concurrently is extensive and results in a high risk that security problems could go undetected. In addition, in the case of the STIR security testing, tests had to be re-performed and the certification

⁸ Integration testing is the process of ensuring that all components (hardware and software) are working correctly within a system and collectively with all other systems.

⁹ Site readiness testing involves determining if all elements are ready at each physical location containing any component of the new system.

¹⁰ Configuration management involves identifying critical project items (documents, software, and hardware), controlling changes to those items, and recording and reporting any changes to the items.

¹¹ Regression testing is the process of identifying any changes to previously working computer functions after modifications have been performed.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

process repeated several times to ensure security requirements were still in compliance. The cost for consultants performing security testing for the STIR was over \$356,000.

Security test results were not always accurately reported

As stated earlier, a key component of the certification package is the report of security testing results. We found several inaccuracies in this report that could raise questions about its reliability.

For example, the CPO did not disclose all significant results from the STIR security tests. The results from 14 cases that did not pass during testing were omitted from the report. In addition, several test case results were contradictory and did not provide the necessary evidence to validate that the security requirements were met.

When we discussed this with CPO management, they indicated that they inadvertently did not disclose these failed or incomplete test results, and that they were working to improve this in the security testing for the next release of modernized systems.

Not appropriately disclosing testing results will prevent senior management and executives from having all the data necessary to make informed decisions and to ensure that all mitigating controls are in place. This practice undermines the integrity and reliability of processes used to provide security certification and accreditation for all modernized information systems. In addition, this could result in systems being moved into production with security weaknesses that could leave them vulnerable to outside attack or other unauthorized access to taxpayer data.

The failed test cases not reported in the STIR's initial security testing may go undetected in subsequent releases of the STIR and not be retested. It is critical that all failed test cases are reported along with their respective deferrals or mitigation plans. This provides a formal means of accurately tracking those test cases to perform retesting at the appropriate time.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Management Actions: Internal and external penetration testing¹² of the STIR was conducted April 9 through 11 and 15 through 19, 2002, prior to loading any applications onto the infrastructure. The management in the CPO has indicated that the risks associated with unauthorized access were reduced through the penetration testing that was performed.

Recommendations

To reduce security risks for future BSM systems, we recommend that the Acting Deputy Commissioner for Modernization & Chief Information Officer:

3. Ensure that the CPO performs security tests on all physical components of the infrastructure located at each functional site, especially if the number of sites is limited. If the IRS decides in certain instances that this is not feasible, this decision and the associated risks should be communicated clearly within the security testing reports detailing specific components, areas, locations, and reasons why they were not tested.

Management's Response: The Acting Deputy Commissioner for Modernization & Chief Information Officer disagreed with this recommendation. He responded that using NIST Guidance, the IRS certification and accreditation process allows for management to make an informed decision on a project-by-project basis on the testing methodology. For the STIR, the IRS employed Type accreditation. The response also stated that Type accreditation can be used when the same system or configuration is being installed in multiple locations. However, he also stated that clearly communicating the decision and risks will be part of the process improvement activities associated with the ELC. The security test reports will also include system components, areas, locations, and justification for test methodology.

¹² Penetration testing determines whether controls are adequate to detect or deter unauthorized individuals from accessing or "penetrating" a system.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Office of Audit Comment: As we reported earlier, we believe that applying Type accreditation for a system as critical as the infrastructure is inappropriate. We also believe that, while it is inappropriate to apply Type accreditation to the STIR, the IRS relied upon the advantages of that guidance without following or performing the recommended or suggested NIST processes and procedures that should occur to provide the necessary support for a Type accreditation.

4. Require the BSMO to inform the PRIME contractor that alleviating schedule delays by executing security testing concurrently with other critical test phases is not an acceptable practice and should be conducted only in very rare circumstances. If and when the BSMO and the IRS determine circumstances are such that concurrent testing is necessary, these actions and their associated risks should be communicated clearly within the security testing reports.

Management's Response: The Acting Deputy Commissioner for Modernization & Chief Information Officer disagreed that the IRS performed concurrent testing. He responded that the IRS did not and will not allow risky concurrent testing for the STIR. He indicated he believes a system can be tested at the same location and on the same day, but at different times. The response also stated that the IRS security testing process is sequential as it relates to completion of system components and the system. He further stated that the Security Test and Evaluation was not conducted prior to or at the same time as the Deployment Site Readiness or Integration Test.

Office of Audit Comment: We believe that the three test phases of integration, deployment site readiness, and security testing should occur independently and be completed prior to the start of another test phase. This is beneficial because changes are often made to systems based on test results, so all tests should be completed and changes made before a system is submitted for security testing to ensure the final configuration is tested. Although the Acting Deputy Commissioner for Modernization & Chief Information Officer stated that the IRS did not allow

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

concurrent testing to occur for the STIR, the three test phases were performed during the same time period, which we believe is concurrent testing. We maintain that it is a risky practice to perform multiple testing phases on the same system/components on the same day, especially when each test phase can require several weeks to complete.

While the IRS security testing process is sequential as it relates to completion of system components, security testing must also be performed on those system components as an integrated whole to ensure that security configurations of one component do not negate the security configurations of another component. This requires overall system integration testing to be completed before security tests are performed. In the case of the STIR testing, tests had to be re-performed and the certification process repeated several times to ensure security requirements were still in compliance after changes to the system were made.

5. Require the CPO to develop improved processes to ensure that security testing results are accurately and completely disclosed in the security testing report. In addition, documentation listing all failed or inaccurately disclosed test cases from the first release of the STIR's security testing report should be prepared and attached to the security test report for the certification and accreditation of the next release of the infrastructure.

Management's Response: The Acting Deputy Commissioner for Modernization & Chief Information Officer agreed with this recommendation. However, he stated that excluding the commercial-off-the-shelf (COTS) software limitations results from the certification transmittal memorandum did not negatively affect executive decision making because this information was fully disclosed in the risk mitigation plans that they reviewed. As corrective action, he stated that the certification and accreditation processes within the ELC will be enhanced to require the certification transmittal memorandum to include the reporting of information for COTS limitation; and all proposed security test cases, whether performed or not, will be included or accounted for within the final security evaluation.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Critical Infrastructure Documentation Was Not Provided Timely

The CPO uses several different reports provided by the STIR team when developing and planning the infrastructure security tests.¹³ Many of these reports contain the only official specifications available for the CPO and its security consultants to effectively plan the detailed test cases within the security test. The reports list all hardware and software components within the infrastructure describing in detail their configuration and complexities of the system as a whole. However, due to constant changes to the infrastructure deliverables, information within the reports was not accurate and did not present a true and clear picture of the STIR.

We found inconsistencies regarding various STIR components reported in the critical documentation used for security testing. These documents were all dated in late January or mid-February 2002. Because of the inconsistencies, we were not certain of these components' existence, but we did determine that most do not appear to have been tested in the security tests.

When we discussed this issue with BSMO management, they indicated that they were aware of this issue, but due to time pressures, they had to proceed with security testing without having accurate system documentation. Meetings were held with the CPO to alleviate this issue.

Without accurate documentation of the infrastructure, the CPO could not effectively plan for testing the security of all required components, and pre-Security Testing and Evaluation meetings were necessary to determine what components in the Modernization Release were to be tested. As a direct result, the CPO had to deviate from its original security test plan during execution of the security tests. The deviations were needed because hardware and software components originally planned in the reports were moved to a future release.

¹³ Reports include but are not limited to the following: Security Plan, Security Features User's Guide, Configuration Management Plan, Technical Contingency Planning Document, Physical Technology Model, and Data Model View.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

These issues pose a significant risk to the accurate completion of security testing. For example, the interactions between hardware and software components may affect the security of a system based upon the configuration settings. Security settings, if installed improperly on one component, may negate the security settings of all other components within a system, leaving an undetected vulnerability to possible attackers. Therefore, it is critical that accurate and complete information is available when the security test plan is being developed to sufficiently research all possible scenarios.

The security test plan is a required component of the certification process, providing detailed test cases containing verification techniques and procedures for all the components of the STIR. Any unexplained deviations from the security test plan should be reported to ensure the integrity and effectiveness of the certification process. However, the security test report did not include explanations of the deviations that occurred during the testing process.

If system documentation contains inaccurate descriptions of the physical design and make-up of a system, it will be difficult to determine what changes were made in future releases, as required in the post-accreditation phase of the security certification and accreditation process. Without accurate documentation providing the true configuration and design of all existing STIR components, it will be difficult to perform any analysis or comparison to future system changes or provide accountability to the first release.

Management Actions: The CPO has adopted a new process requiring the verification of a system's configuration to be performed and signed before the Security Testing and Evaluation is conducted.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Recommendations

To better enable security test planning and execution, we recommend that the Acting Deputy Commissioner for Modernization & Chief Information Officer:

6. Require the Infrastructure Program Office and the PRIME contractor to produce updated and accurate copies of the critical STIR 1.0 system documentation for use in future system security monitoring, as well as for use by the Information Technology Services organization in maintaining the system.

Management's Response: The Acting Deputy Commissioner for Modernization & Chief Information Officer disagreed with this recommendation. He responded that the STIR is being deployed in various releases and stated that Release 1.0 has been superseded by Release 1.2. STIR 1.2 documentation reflects the current infrastructure. With any future release of the STIR, the documentation will be updated to provide an accurate depiction of the system.

Office of Audit Comment: We concur with the alternative corrective actions stated in Management's Response as long as the updated STIR documentation prepared for each new release includes all existing components from previous releases.

7. Require that accurate and complete system documentation be provided for future systems prior to beginning security testing.

Management's Response: The Acting Deputy Commissioner for Modernization & Chief Information Officer agreed with this recommendation. He responded that the certification and accreditation process will be enhanced to require that a Physical Configuration Audit be performed and approved before Security Test and Evaluation is conducted. He also stated that this configuration audit will identify the components comprising the release and the test will be conducted based on those components. The CPO will clearly document and explain

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

any future deviations from the security test plan in the security test report.

8. Require the CPO to clearly explain any future deviations from the security test plan in the security test report.

Management's Response: The Acting Deputy Commissioner for Modernization & Chief Information Officer agreed with this recommendation. He responded that the enhanced certification and accreditation processes within the ELC would require documentation of all results from the security test plan in the security test report.

Detailed Objective, Scope, and Methodology

The objective of this review was to determine the adequacy and effectiveness of security testing performed on the Internal Revenue Service's (IRS) Security and Technology Infrastructure Release (STIR) 1.0.

To accomplish this objective, we determined whether key security features of the modernized infrastructure¹ and its interfaces were tested prior to implementation. Specifically, we:

- A. Obtained an understanding of the security certification and accreditation² processes for modernization projects.
- B. Obtained and documented an understanding of the applicable laws and regulations affecting each system in regard to information systems security.
- C. Reviewed the management organizational structure and met with the Director of Modernization Security as well as the Infrastructure Director to determine information systems security responsibilities between the IRS and the PRIME contractor.³
- D. Evaluated security testing documentation for the STIR to determine whether this testing adequately covered the information systems security environment.
- E. Reviewed the security processes performed for the addition of an existing application to the STIR Infrastructure.

¹ Infrastructure refers to the hardware, software, and security systems that computer systems use to communicate and share information.

² Certification requires a comprehensive evaluation of technical and nontechnical security features to determine the extent to which system design and implementation meet a specified set of security requirements. Accreditation is an official declaration by the responsible official (i.e., system owner) that an information system or network is approved to operate with prescribed security safeguards.

³ The PRIME contractor is the Computer Sciences Corporation, which heads an alliance of leading technology companies assisting the IRS with modernizing its computer systems and related technology.

Major Contributors to This Report

Margaret E. Begg, Acting Assistant Inspector General for Audit (Information Systems Programs)

Gary V. Hinkle, Director

Scott A. Macfarlane, Director

Tammy Whitcomb, Audit Manager

Michelle Griffin, Senior Auditor

Bret Hunter, Senior Auditor

Phung Son Huu Nguyen, Senior Auditor

**Security Testing and Certification of the Modernized Infrastructure
Needs to Be Strengthened**

Appendix III

Report Distribution List

Commissioner N:C
Deputy Commissioner for Operations Support N:DC
Associate Commissioner, Business Systems Modernization M:B
Chief, Information Technology Services M:I
Chief, Security Services M:S
Deputy Associate Commissioner, Systems Integration M:B:SI
Director, Mission Assurance M:S:A
Director, Modernization Security M:S:M
Director, Portfolio Management M:R:PM
Chief Counsel CC
National Taxpayer Advocate TA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Office of Management and Controls N:CFO:AR:M
Audit Liaisons:
 Associate Commissioner, Business Systems Modernization M:B
 Chief, Information Technology Services M:I

**Security Testing and Certification of the Modernized Infrastructure
Needs to Be Strengthened**

Appendix IV

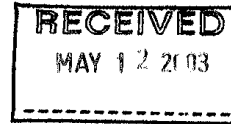
Management's Response to the Draft Report



DEPUTY COMMISSIONER


DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

MAY 9 2003



MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX
ADMINISTRATION

FROM:


Dave A. Mader
Acting Deputy Commissioner for Modernization &
Chief Information Officer

Subject:

Draft Audit Report - Security Testing and Certification of the
Modernized Infrastructure Needs to Be Strengthened
(Audit # 200320036)

Thank you for your draft audit report that acknowledges that STIR Release 1.0 was a monumental step in providing opportunities for the development and deployment of all other modernized projects. The Security and Technology Infrastructure (STIR) project was designed to provide a fully secure computing environment based upon web technology utilizing the Internet as a primary means for communicating and delivering taxpayer information. Specifically, the project has:

- Delivered a fully integrated, shared information technology infrastructure which includes hardware, software, shared applications and data, telecommunications, and security.
- Provided an enterprise-wide approach to systems and operations management that will yield cost savings in developing, deploying, and maintaining the infrastructure of the modernized environment.

IRS concurs with your findings that we need to provide timely and formal documentation during the security certification testing and accreditation process. Your observations are consistent with continuing IRS actions to strengthen its security certification capabilities and to safeguard taxpayer data. There are, however, additional findings with which we do not concur. The specifics are provided below. In addition, we are attaching a detailed response to each of your report recommendations.

Certification and Accreditation Processes Were Not Completed Until Several Months After Project Deployment

IRS does not concur with the finding that the STIR certification process was not completed until months after the system became operational. During the course of the

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

2

audit, we provided the audit team with information that documented the certification was completed prior to deployment, based on an unconditional certification memorandum. *Specifically, the certification transmittal memorandum, dated May 1, 2002, unconditionally certified the Modernization Release 1 of STIR until May 1, 2005 and the system was deployed that same day.* The certification memorandum package contained completed security test results, a mitigation strategy that assessed residual risks, and a list of the security test and evaluation findings that would be deferred to the next release of STIR, that is Release 1.2. The package indicated that the contractor's Security Evaluation Report and Certification Statement would be forthcoming. IRS executives fully engaged in the certification and accreditation processes, assessed this risk, and the CIO approved the STIR for operation. A copy of the certification transmittal memorandum is attached.

The final certification transmittal memorandum was issued on October 25, 2002. The memorandum package was issued to include the contractor's formal deliverable--the Security Evaluation Report and the Certification Statement. The security results in the interim certification memorandum, which included the findings, mitigation strategy, resolutions, and deferred findings for a subsequent release, remained the same in the final certification memorandum.

Limitations of Security Testing and Inaccurate Reporting

IRS does not concur with the findings that security testing was limited, concurrent, or that test results were inaccurately reported. *The Certification Program Office (CPO) conducted an independent security test to verify and validate STIR's security functionality against IRS' security requirements. Test results were accurately reported.*

IRS employed "type accreditation" for STIR. Type accreditation can be used when the exact same system or configuration is being installed in multiple locations. The NIST Guidelines for the Security Certification and Accreditation of Federal Information System states "to support type accreditations of major applications and general support systems, initial security testing and evaluation, sometimes referred to as developmental Security Test and Evaluation (ST&E), *should occur*, at a central integration and test facility or at one of the intended operating sites, if a test facility is not available. Software and hardware security testing of common system components at multiple sites is not recommended. The site will not need to repeat the baseline ST&E conducted during the type accreditation. However, the system installation and security configuration *should be tested* at each operation location during operational (or site) ST&E." The Registered User Portals, used to obtain access to STIR, have identical hardware, software, firmware and configuration at the multiple locations; therefore, we used type accreditation methodology to accredit this general support system.

As noted in your draft report, penetration tests were performed. However, the draft report does not adequately consider this information when reporting that security tests were limited. The penetration tests are key and critical tests that determine whether controls are adequate to detect and deter unauthorized accesses. Both internal and

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

3

external penetration tests were conducted during April 2002. The internal and external penetration tests included (1) using well known hacking techniques to identify security vulnerabilities, and (2) attempting to exploit common security vulnerabilities. Reported results of the penetration tests denoted that no vulnerabilities were identified. For example, external Internet users are unable to connect to the STIR' resources or determine the type and version of the web server software and operating system being used. *The STIR External Penetration Testing Report, dated April 11, 2002, and the STIR Internal Penetration Testing Report, dated April 23, 2002, were completed prior to issuing the Certification Transmittal Memorandum granting interim security certification to the STIR project.* We are emphasizing that these tests were completed prior to installing any applications onto the IRS infrastructure.

IRS did not allow risky concurrent testing as the report indicates. The IRS' security testing process provides for sequential testing. A system can be tested at the same location, on the same day, but at different times. ST&E tests were not conducted prior to or at the same time as the Deployment Site Readiness Test (DSRT) or Integration Test. In addition, regression testing was performed. This process identifies any changes to previously working computer functions, after modifications are performed, to ensure that documented findings were corrected. During regression testing for STIR Release 1.0, no additional findings were detected.

All security test results were accurately reported. The process used at the time of the audit did not require that the Certification Transmittal Memorandum include the reporting of limitations from commercial off-the-shelf (COTS) products. Excluding the COTS limitations results from the certification transmittal memorandum did not negatively impact executive decision-making because this information was fully disclosed in the risk mitigation plans that they reviewed. However, based on the audit observation, the process will be enhanced to include in the certification transmittal memorandum the reporting of information for COTS limitations.

Critical Infrastructure Documentation Was Not Provided Timely

By "timely" the following is assumed to be meant: The scope of the system deployed is less than the documentation describing the system. The STIR project was separated into two releases but the documentation was one comprehensive package for both releases, with additions/corrections being made for the future STIR Releases. As requirements were annotated and further defined, issues that were identified in STIR Release 1.0 were deferred and accomplished in STIR Release 1.2. The deviations were needed because hardware/software components, originally planned in the reports, were moved to a future release. To mitigate this and to verify that the security test plan adequately tests all components of the deployed system, the process will be improved to include requiring that a Physical Configuration Audit is performed and approved before Security Test and Evaluation is conducted. This configuration audit will identify the components comprising the release and the test is conducted based on those components. The CPO will also clearly document and explain any future deviations from the security test plan in the security test report.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

4

If you have any questions, please contact me at (202) 622-4700, or Colleen Murphy, Acting Chief, Security Services at (202) 622-8910.

Attachments

cc: Associate Commissioner, Business Systems Modernization
Director, Mission Assurance
Director, Modernization Security
Director, Security Policy Support and Oversight

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened (Audit # 200320036)

Report Section: Limitations Of Security Testing And Inaccurate Reporting Of Results Could Increase Project Risks

RECOMMENDATION #1: To ensure that future BSM projects meet security requirements and IRS officials clearly understand risks related to the projects and the impacts on their operations, we recommend that the Deputy Commissioner for Modernization & Chief Information Officer ensure that security certification and accreditation is performed with all formal documents completed and approved prior to allowing any future BSM project to process sensitive taxpayer data.

CORRECTIVE ACTION #1:

The IRS certification and accreditation process allows for an informed management decision to be made on a project-by-project basis that considers the project risks at the completion of the security test and evaluation. If there is an immediate business need and risks are moderate to low, IRS management may proceed to authorize processing. Accreditation paperwork will follow as soon as possible. The improved certification and accreditation within the Enterprise Life Cycle process will indicate what document is needed that communicates this authority.

IMPLEMENTATION DATE:

September 1, 2003

RESPONSIBLE OFFICIAL:

Director, Mission Assurance (M:S:A)

CORRECTIVE ACTION MONITORING PLAN:

Requirements indicated throughout the phases of the Enterprise Life Cycle process are reviewed at each appropriate milestone.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened (Audit # 200320036)

Report Section: Certification And Accreditation Processes Were Not Completed Until Several Months After Project Deployment

RECOMMENDATION #2: To ensure that future BSM projects meet security requirements and IRS officials clearly understand risks related to the projects and the impacts on their operations, we recommend that the Deputy Commissioner for Modernization & Chief Information Officer review the Enterprise Life Cycle to determine if the guidance related to security requirements prior to authorizing deployment of a system is accurate. If not, request immediate changes to the Enterprise Life Cycle to ensure future projects are following correct guidance.

CORRECTIVE ACTION #2:

The Security Test and Evaluation must occur in the deployed environment following the Deployment Site Readiness Test. The test, and the resulting Security Evaluation Report, cannot be addressed in the development phase (Milestone 4 of the Enterprise Life Cycle). It must be completed in the deployment phase (Milestone 5). Actions are underway to enhance the documentation, timing related to milestones, and the timing of security tests within the Enterprise Life Cycle process.

IMPLEMENTATION DATE:

September 1, 2003

RESPONSIBLE OFFICIAL:

Director, Modernization Security (M:S:M)

CORRECTIVE ACTION MONITORING PLAN:

A tabletop exercise will be conducted no-later-than September 30, 2003.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened (Audit # 200320036)

Report Section: Limitations of Security Testing and Inaccurate Reporting Of Results Could Increase Project Risks

RECOMMENDATION #3: To reduce security risks for future BSM systems, we recommend that the Deputy Commissioner for Modernization & Chief Information Officer ensure that the CPO performs security tests on all physical components of the infrastructure located at each functional site, especially if the number of sites is limited. If the IRS decides in certain instances that this is not feasible, this decision and the associated risks should be communicated clearly within the security testing reports detailing specific components, areas, locations, and reasons why they were not tested.

CORRECTIVE ACTION #3:

Using NIST Guidance, the IRS certification and accreditation process allows for management to make an informed decision on a project-by-project basis on the testing methodology. For STIR Release 1.0, IRS employed "type accreditation". Type accreditation can be used when the exact same system or configuration is being installed in multiple locations. We continue to support the decision to perform "type accreditation" for STIR Release 1.0.

Clearly communicating the decision and risks will be part of the process improvement activities associated with the Enterprise Life Cycle. The security test reports will also include system components, areas, locations, and justification for test methodology.

IMPLEMENTATION DATE:

September 1, 2003

RESPONSIBLE OFFICIAL:

Director, Mission Assurance M:S:A

CORRECTIVE ACTION MONITORING PLAN:

Requirements indicated throughout the phases of the Enterprise Life Cycle process are reviewed at each appropriate milestone.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened (Audit # 200320036)

Report Section: Limitations of Security Testing and Inaccurate Reporting Of Results Could Increase Project Risks

RECOMMENDATION #4: To reduce security risks for future BSM systems, we recommend that the Deputy Commissioner for Modernization & Chief Information Officer require the BSMO to inform the PRIME contractor that alleviating schedule delays by executing security testing concurrently with other critical test phases is not an acceptable practice and should only be conducted in very rare circumstances. If and when the BSMO and the IRS determine circumstances are such that concurrent testing is necessary, these actions and their associated risks should be communicated clearly within the security testing reports.

CORRECTIVE ACTION #4:

No action required. IRS did not and will not allow risky concurrent testing as the report indicates had occurred for STIR Release 1.0. The IRS security testing process is sequential as it relates to completion of system components and the system. A system can be tested at the same location, on the same day, but at different times. The Security Test and Evaluation was not conducted prior to or at the same time as the Deployment Site Readiness Test or Integration Test.

IMPLEMENTATION DATE:

April 1, 2003

RESPONSIBLE OFFICIAL:

Director, Mission Assurance M:S:A

CORRECTIVE ACTION MONITORING PLAN: N/A

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened (Audit # 200320036)

Report Section: Limitations of Security Testing and Inaccurate Reporting Of Results Could Increase Project Risks

RECOMMENDATION #5: To reduce security risks for future BSM systems, we recommend that the Deputy Commissioner for Modernization & Chief Information Officer require the CPO to develop improved processes to ensure that security-testing results are accurately and completely disclosed in the security testing report. In addition, documentation listing all failed or inaccurately disclosed test cases from the first release of the STIR's security testing report should be prepared and attached to the security test report for the certification and accreditation of the next release of the infrastructure.

CORRECTIVE ACTION #5:

During the time of this audit, the certification and accreditation process did not require that the Certification Transmittal Memorandum include the reporting of limitations from commercial off-the-shelf (COTS) products. Excluding the COTS limitations results from the certification transmittal memorandum did not negatively impact executive decision-making because this information was fully disclosed in the risk mitigation plans that they reviewed. The certification and accreditation process within the Enterprise Life Cycle will be enhanced to require that the certification transmittal memorandum include the reporting of information for COTS limitations; and all proposed security test cases, whether performed or not, will be included or accounted for within the final security evaluation.

IMPLEMENTATION DATE:

September 1, 2003

RESPONSIBLE OFFICIAL:

Director, Mission Assurance M:S:A

CORRECTIVE ACTION MONITORING PLAN:

Requirements indicated throughout the phases of the Enterprise Life Cycle process are reviewed at each appropriate milestone.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened (Audit # 200320036)

Report Section: Critical Infrastructure Documentation Was Not Provided Timely

RECOMMENDATION #6: To better enable security test planning and execution, we recommend that the Deputy Commissioner for Modernization & Chief Information Officer require the Infrastructure Program Office and the PRIME contractor to produce updated and accurate copies of the critical STIR 1.0 system documentation for use in future system security monitoring, as well as for use by the Information Technology Services organization in maintaining the system.

CORRECTIVE ACTION #6:

No action required. STIR is being deployed in various releases. STIR Release 1.0 has been superseded by Release 1.2. With any future release of STIR, the documentation will be updated to provide an accurate depiction of the system. STIR Release 1.2 documentation reflects the current infrastructure.

IMPLEMENTATION DATE:

April 1, 2003

RESPONSIBLE OFFICIAL:

Director, Mission Assurance (M:S:A)

CORRECTIVE ACTION MONITORING PLAN: N/A

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened (Audit # 200320036)

Report Section: Critical Infrastructure Documentation Was Not Provided Timely

RECOMMENDATION #7: To better enable security test planning and execution, we recommend that the Deputy Commissioner for Modernization & Chief Information Officer require that accurate and complete system documentation be provided for future systems prior to beginning security testing.

CORRECTIVE ACTION #7:

By "timely" the following is assumed: The scope of the system deployed is less than the documentation describing the system. The STIR project was separated into two releases, but the documentation was one comprehensive package for both releases. As requirements were annotated and further defined, issues that were identified in STIR Release 1.0 were deferred and accomplished in STIR Release 1.2. The deviations were needed because hardware/software components originally planned in the reports were moved to a future release.

To mitigate this and to verify that our security test plan adequately tests all components of the deployed system, the certification and accreditation process will be enhanced to require that a Physical Configuration Audit is performed and approved before Security Test and Evaluation is conducted. This configuration audit will identify the components comprising the release and the test is conducted based on those components. The CPO will also clearly document and explain any future deviations from the security test plan in the security test report.

IMPLEMENTATION DATE:

September 1, 2003

RESPONSIBLE OFFICIAL:

Director, Mission Assurance (M:S:A)

CORRECTIVE ACTION MONITORING PLAN:

Requirements indicated throughout the phases of the Enterprise Life Cycle process are reviewed at each appropriate milestone.

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened

Security Testing and Certification of the Modernized Infrastructure Needs to Be Strengthened (Audit # 200320036)

Report Section: Critical Infrastructure Documentation Was Not Provided Timely

RECOMMENDATION #8: To better enable security test planning and execution, we recommend that the Deputy Commissioner for Modernization & Chief Information Officer require the Certification Program Office to clearly explain any future deviations from the security test plan in the security test report

CORRECTIVE ACTION #8:

The enhanced certification and accreditation process within the Enterprise Life Cycle will require documentation of all results from the security test plan in the security test report.

IMPLEMENTATION DATE:

September 1, 2003

RESPONSIBLE OFFICIAL:

Director, Mission Assurance (M:S:A)

CORRECTIVE ACTION MONITORING PLAN:

Requirements indicated throughout the phases of the Enterprise Life Cycle process are reviewed at each appropriate milestone.

**Security Testing and Certification of the Modernized Infrastructure
Needs to Be Strengthened**



DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

May 1, 2002

MEMORANDUM FOR CHIEF, INFORMATION TECHNOLOGY SERVICES

FROM:


John C. Reece
Deputy Commissioner for Modernization and
Chief Information Officer

SUBJECT:

Unconditional Security Certification Transmittal for
Modernization Release 1 of Security Technological
Infrastructure Release (STIR)

Based on the recommendation from the Certification Program Office (M:S:A:C) authorizing immediate interim approval to operate, I am unconditionally certifying the Modernization Release 1, Security Technological Infrastructure Release until May 1, 2005. Attached is the mitigation strategy addressing specific information to assess the residual risk and a list of the Security Test and Evaluation Findings Deferred to Release 1.2. Please remember, personnel responsible for using or operating this system need to adhere to the certified system configuration and procedures to maintain this interim certification. In this regard, changes to this certified configuration need to be coordinated with Mission Assurance to maintain the certification and to ensure the confidentiality, integrity and availability of its data.

The Security Test and Evaluation was completed on April 25, 2002. The formal Certification Transmittal Memorandum, Certification Statement, and Security Evaluation Report will be submitted for signature within two weeks of this immediate interim approval.

If you have any questions, please contact Len Baptiste, Chief, Security Services at (202) 622-8910, or a member of your staff can contact George Jakabcin, Director, Modernization Security, at (202) 622-4097.

Attachments (2)