

DOE/IG-0569

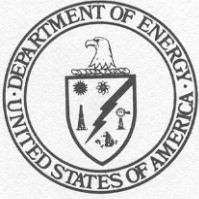
EVALUATION
REPORT

THE FEDERAL ENERGY
REGULATORY COMMISSION'S
UNCLASSIFIED CYBER SECURITY
PROGRAM 2002



SEPTEMBER 2002

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF AUDIT SERVICES



Department of Energy


Washington, DC 20585

September 13, 2002

MEMORANDUM FOR THE CHAIRMAN

FEDERAL ENERGY REGULATORY COMMISSION

FROM:


Gregory H. Friedman
Inspector General

SUBJECT:

INFORMATION: Evaluation Report on "The Federal Energy
Regulatory Commission's Unclassified Cyber Security Program 2002"

BACKGROUND

The Federal Energy Regulatory Commission (Commission) increasingly relies on information technology systems as it carries out its mission to regulate the transmission and sale of electric power, natural gas, oil, and hydroelectric power. The Commission expects to invest \$23 million in information technology related activities in Fiscal Year 2002 as it moves toward satisfying the President's Management Agenda goal of significantly enhancing electronic government.

Congress enacted the Government Information Security Reform Act (GISRA) in October 2000 to codify existing policies and regulations and reiterate security responsibilities outlined in the Computer Security Act of 1987 and the Clinger-Cohen Act of 1996. GISRA focuses on program management, implementation, and evaluation aspects of the security of government information and requires agencies to conduct annual program reviews and independent evaluations of computer security programs.

As required by GISRA and Office of Management and Budget implementing guidance, the Office of Inspector General performed an evaluation to determine whether the Commission's cyber security program protected data and information systems.

RESULTS OF EVALUATION

The Commission had implemented a number of protective measures, but certain critical information systems remained at risk. Cyber protection efforts suffered from program management, planning, and execution weaknesses. Specifically, the Commission had not developed system specific security plans; adequately planned for contingency and disaster recovery; implemented a completely effective cyber security training program; or adequately addressed configuration management and access control problems.

Vulnerabilities existed because the Commission had not provided adequate management attention to implementing an effective cyber security program. As a result, the Commission's systems were at risk of unauthorized or malicious use and the potential for compromise of



sensitive operational and personnel-related data was increased. We recommended that the Commission clarify roles and authorities relative to its cyber security protection program and that it establish performance goals and metrics to measure progress in improving cyber security throughout the agency.

MANAGEMENT REACTION

Management concurred with our recommendations and stated that it had addressed many observations identified in the report by enhancing certain elements of the cyber security program. Management also stated that it planned to work over the course of the next year to close evaluation findings through corrective action plans.

Attachment

cc: Executive Director and Chief Financial Officer, FERC
Chief Information Officer, FERC
Chief of Staff, Department of Energy

THE FEDERAL ENERGY REGULATORY COMMISSION'S CYBER SECURITY PROGRAM 2002

TABLE OF CONTENTS

Overview

Introduction and Objective.....	1
Conclusions and Observations.....	1

Cyber Security Program Weaknesses

Details of Finding.....	3
Recommendations and Comments	7

Appendices

1. Scope and Methodology	8
2. Related Reports	9
3. Management Comments.....	10

Overview

INTRODUCTION AND OBJECTIVE

The Department of Energy (Department) Organization Act established the Federal Energy Regulatory Commission (Commission) in 1977. The Commission is an independent entity within the Department that regulates the transmission and sale of electric power, natural gas, oil, and hydroelectric power. The Commission's increasing reliance on information technology systems is consistent with satisfying the President's Management Agenda initiative of expanding electronic government. Specifically, the Commission expects to invest \$23 million in information technology-related activities in Fiscal Year 2002. This substantial investment supports the development and maintenance of diverse information systems used to meet day-to-day mission requirements such as financial management, utility regulation, and licensing of hydroelectric projects.

Congress enacted the Government Information Security Reform Act (GISRA) in October 2000 to codify existing policies and regulations and reiterate security responsibilities outlined in the Computer Security Act of 1987 and the Clinger-Cohen Act of 1996. GISRA focuses on program management, implementation, and evaluation aspects of the security of government information and requires agencies to conduct annual program reviews and independent evaluations of computer security programs.

As required by GISRA and Office of Management and Budget (OMB) implementing guidance, the Office of Inspector General (OIG) performed an evaluation to determine whether the Commission's cyber security program protected data and information systems.

CONCLUSIONS AND OBSERVATIONS

While the Commission had implemented a number of protective measures, certain critical information systems remained at risk. Cyber protection efforts suffered from program management, planning, and execution weaknesses. Specifically, we noted that the Commission had not:

- developed system specific security plans;
- assured continuity of operations through adequate contingency and disaster recovery planning;
- implemented a completely effective cyber security training program; and
- adequately addressed certain configuration management and access control problems.

These vulnerabilities existed because the Commission had not provided adequate management attention to implementing an effective cyber security program. These problems placed the Commission's systems at risk of unauthorized or malicious use and increased the potential for compromise of sensitive operational and personnel-related data.

The Commission has taken several positive steps in an effort to strengthen its cyber security program. The Office of the Chief Information Officer (CIO) recently instituted procedures to review and strengthen network passwords. The CIO is also in the process of developing policies and procedures that should provide the framework for a more fully developed cyber security program. In addition, an Agency Plan of Action and Milestones database has been developed to track cyber security weaknesses and related corrective actions. The Commission is also working to develop and finalize an organization-wide Cyber Security Action Plan. While program improvements have occurred, additional work is necessary to ensure that critical information technology resources are adequately protected.

Due to security considerations, information on specific vulnerabilities and systems has been omitted from this report. Management officials have been provided with detailed information regarding identified vulnerabilities, and in some instances, have initiated corrective actions.

This audit identified issues that management should consider when preparing its year-end assurance memorandum on internal controls.

(Signed)
Office of Inspector General

Cyber Security Program Weaknesses

Systems and Data Remain at Risk

The Commission's cyber security program did not adequately protect information systems resources and data. Specifically, security plans had not always been prepared to mitigate risks or known vulnerabilities for specific systems. In addition, continuity of operations plans had not been developed and tested to permit quick recovery from a security-related system failure. Furthermore, the Commission had not ensured that staff and individuals with significant security responsibilities had received adequate cyber security training. Configuration management and access control weaknesses also increased the risk of malicious or unauthorized access to networks and systems.

System Security Planning

While the Commission contracted with an independent entity to perform a vulnerability assessment on its information systems, we found that a system specific security plan addressing operational risks and remediation approaches had only been developed for one major system. Plans remained incomplete despite the identification of this issue during the Fiscal Year 2001 Financial Statement Audit. Although the Commission had not completed such plans, it had taken the incremental step of conducting an evaluation of its systems using the National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. However, at the time of our review, the Commission had only completed self-assessments on approximately 50 percent of its systems.

Even though action had been taken to improve cyber security planning, additional steps are needed. Specifically, the Commission's Cyber Security Action Plan remained in draft and did not include all of the elements necessary for ensuring its effectiveness. For example, the draft plan did not include milestone dates critical to securing the information technology environment. In addition, a prioritized list of systems the Commission could use to identify mission critical¹ systems had not been developed.

Continuity Planning

Continuity of operations plans to permit quick recovery from a security-related system failure or disruption of critical services were not in place. We noted that both organization-wide and systems specific

¹We considered a system to be mission critical if, in our opinion, it met the definition found in Section 3532(b)(2)(C), GISRA, i.e., if it "processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency."

contingency plans had not been developed or had not been approved. While the Commission had taken action to mitigate the risk of system failure by creating and storing computer data backup tapes off-site, it had not tested the ability to restore such data at alternate processing sites. Failure to develop and test such plans exposes the Commission to the risk that it would be unable to restore critical networks and information systems or maintain continuity of operations in the event of a successful attack.

Training

The Commission's cyber security training program was also not completely effective. While the Commission was proactive in providing cyber security awareness training, it had not focused sufficient attention on those individuals with significant security responsibilities. Specifically, at the time of our evaluation, the Commission had not identified the universe of such employees or developed a core curriculum for them.

Configuration Management and Access Controls

Configuration management weaknesses at the Commission presented opportunities for malicious access by both internal and external entities and increased the potential for unauthorized changes or damage to software and data. For example, outdated software with known vulnerabilities was observed on 11 servers. We also found improperly configured or unsecured remote access and file transfer services on numerous servers. Additionally, several system servers were configured in a manner that could permit unauthorized access for changing or obtaining information. The risk of malicious or unauthorized access was exacerbated by the fact that software tools installed on several systems did not permit auditing and monitoring of unusual or potentially harmful system activity.

Weak access controls and poor password management also increased the risk of unauthorized access. For instance, the Commission did not always employ strong password controls to minimize the risks associated with exploits such as automated guessing or "cracking" programs. One system we evaluated did not require strong passwords that contained an alphanumeric combination. Account access was allowed without passwords for certain systems, including an administrator account that could be used to access multiple servers.

Several other systems did not require that passwords be changed at regular intervals. An important control designed to prevent "brute force" access through password guessing -- account lockout after numerous incorrect login attempts -- had not been activated on one server.

Protection of Information Resources

GISRA requires that each agency develop and implement an agency-wide cyber security program, consisting of policies, procedures, and control techniques, sufficient to protect information systems supporting agency operations and assets. GISRA focuses on program management, implementation, and evaluation aspects of the security of unclassified and national security information. It requires agencies to adopt a risk-based, life cycle approach to improving computer security and requires annual agency information security program reviews and independent evaluations of both unclassified and classified computer security programs. Specifically, GISRA requires:

- Periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems and data;
- Policies and procedures that are based on risk assessments that cost-effectively reduce information security risk to an acceptable level;
- Adequate training of staff responsible for cyber security;
- Cyber security awareness training for agency personnel;
- Periodic management testing and evaluation of the effectiveness of the program;
- A process for ensuring remedial action to address significant deficiencies; and,
- Procedures for detecting, reporting, and responding to cyber security incidents.

Program Design and Implementation

Vulnerabilities existed because the Commission had not provided adequate management attention to implementing an effective cyber security program. Specifically, organizational responsibilities had not been stressed sufficiently and performance measures for cyber security had not been developed.

We identified instances where Commission management was either unaware of responsibilities, uncertain of their authorities, or had not coordinated effectively to ensure that needed actions were taken. For example,

-
- Although the Commission's interim directive for information technology security specifically assigned responsibility for developing and implementing system security plans to office directors, only one office had prepared such a plan. In addition, the one plan that had been prepared was not approved because the head of the office was not aware that it was his responsibility to approve it.
 - During the period under evaluation, officials from the Office of the CIO indicated that they lacked the authority for monitoring or administering security for all of the Commission's financial systems. For example, they noted that they had no authority to conduct testing or review security practices and were not aware of financial information system security weaknesses disclosed by our Fiscal Year 2001 Financial Statement Audit until several months after they were reported.
 - In another instance, we observed that senior management officials did not agree on the identification of mission critical systems and commensurate protective measures. As a result, at the time of our review, the Commission had not identified which systems were critical to continuing operations of the agency.
 - Budgets for cyber security related activities were either not prepared or lacked sufficient specificity to determine whether they addressed individual system lifecycle security costs.

The Commission also had not developed and implemented cyber security related performance goals as required by the Government Performance and Results Act of 1993 (GPRA). The Commission acknowledged the lack of such measures in its 2001 GISRA submission to the OMB but has yet to develop a method for tracking progress in this important area. For instance, specific measures and a metric system capable of measuring progress in areas, such as agency-wide security planning, including security training, and a certification and accreditation process, had not been implemented. While the Commission was tracking performance measurement weaknesses in its Plan of Action and Milestones database, corrective actions related to the development of such measures were not ranked as a high priority and had not been completed.

Risk of Compromise

The threat of compromise of critical information resources continues to grow as the Commission moves closer to a paperless environment. A lack of attention to implementing an effective cyber security program and not promptly correcting weaknesses identified during the FY 2001 GISRA process increased the risk of compromise or malicious damage of the Commission's critical systems, some of which enable delivery of essential services to industry, members of the public, and other Federal agencies. In addition, a lack of cyber security training increases the risk that adequate measures will not be taken to protect the information included in the agency's systems.

RECOMMENDATIONS

To improve cyber security within the Commission, we recommend that the Chairman:

1. Clarify roles and authorities for the CIO related to the development and implementation of a Commission-wide cyber security protection program;
2. Ensure that system security plans are approved, mission critical systems are identified, and that continuity of operations for the systems is assured through adequate contingency and disaster recovery planning;
3. Ensure that cyber security objectives are given appropriate priority within the agency and cyber security costs are included in the system development life cycle; and
4. Direct the establishment of performance goals, and an associated metrics system, for measuring progress in improving cyber security and correcting known weaknesses.

MANAGEMENT REACTION

Management concurred with our recommendations and stated that it had addressed many observations identified in the report by enhancing certain elements of the cyber security program. Management also stated that it planned to work over the course of the next year to close evaluation findings through corrective action plans. The Commission's verbatim comments can be found in Appendix 3.

AUDITOR COMMENTS

Management's comments were responsive to our recommendations.

Appendix 1

SCOPE

Between June and August 2002 we performed a vulnerability assessment of the Commission's cyber security program. Specifically, we assessed controls over network operations to determine the effectiveness of access controls related to safeguarding information resources from unauthorized internal and external sources. The evaluation included a limited review of general and application controls in areas such as entity-wide security planning and management, access controls, application software development and change controls, and service continuity. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls.

METHODOLOGY

We satisfied our evaluation objective by reviewing applicable laws and regulations pertaining to cyber security and information technology resources, such as GISRA, OMB Circular A-130 (Appendix III), and the Clinger-Cohen Act, and reviewing the Commission's overall cyber security program management, policies, procedures, and practices. The Commission's headquarters was evaluated in conjunction with the annual audit of the Department's Consolidated Financial Statements, utilizing work performed by KPMG LLP, the OIG contract auditor. The evaluation included analysis and testing of general and application controls for systems as well as vulnerability and penetration testing of networks.

We evaluated the Commission's implementation of GPRA related to the establishment of performance measures for cyber security. We did not rely solely on computer-processed data to satisfy our objectives. However, computer-assisted audit tools were used to perform probes of various networks and devices. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel and performed other procedures to satisfy ourselves as to the reliability and competence of the data produced by the tests. Because our evaluation was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our evaluation.

The evaluation was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the objectives. We held an exit conference with management on September 10, 2002.

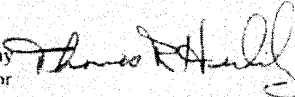
RELATED OFFICE OF INSPECTOR GENERAL AND GENERAL ACCOUNTING OFFICE REPORTS

- *The Department's Unclassified Cyber Security Program*, (DOE/IG-0519, August 2001). While the Department has initiated certain actions designed to enhance cyber security, it has not made sufficient progress in identifying and developing protective measures for critical infrastructures or assets. For example, our audit disclosed that: 1) the identification of national priority assets had not been finalized and the specific identification of critical cyber-related assets had not begun; 2) corrective actions to address issues disclosed by our previous audit of the Department's infrastructure protection program were progressing slowly and remained incomplete; 3) specific, quantifiable infrastructure protection-related performance measures had not been developed; and 4) the Department's critical infrastructure protection plan had not been updated.
- *The Department of Energy's Implementation of the Clinger-Cohen Act of 1996*, (DOE/IG-0507, June 2001). While the Department has taken action to address certain information technology related management problems, it has not been completely successful in implementing the requirements of the Clinger-Cohen Act of 1996. We attributed the problems identified, in part, to the Department's decentralized approach to information technology management and the organizational placement of the CIO.
- *Fiscal Year 2000 Consolidated Financial Statements*, (DOE/IG-FS-01-01, February 2001). The report identified three reportable weaknesses in the Department's system of internal controls pertaining to performance measures, financial management, and unclassified information system security. Specifically, performance goals, in many cases, were not output or outcome oriented and/or were not meaningful, relevant, or stated in objective or quantifiable terms. The Department also had certain network vulnerabilities and general access control weaknesses.
- *Executive Guide: Maximizing the Success of Chief Information Officers: Learning From Leading Organizations*, (GAO-01-376G, February 2001). The General Accounting Office (GAO) issued this executive guide to provide pragmatic guidance that federal agencies can consider in determining how best to integrate CIO functions into their respective organizations. The guide provided critical success factors that, if implemented, will be useful towards achieving a successful information technology environment.
- *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, (GAO/AIMD-00-295, September 2000). GAO noted that a major contributing factor to the existence of security vulnerabilities was ineffective and inconsistent information technology security management throughout the Department. GAO found that, among other things, the Department had not prepared federally required security plans, effectively identified and assessed information security risks, or fully and consistently reported security incidents.

MANAGEMENT COMMENTS

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

Office of the
Executive Director

FROM: Thomas R. Herlihy 
Executive Director

TO: Director, Science, Energy, Technology and Financial Audits
Department of Energy
Office of Inspector General
Office of Audit Services

SUBJECT: Federal Energy Regulatory Commission Cyber Security Program 2002
Evaluation Report

DATE: September 10, 2002

We concur with the four recommendations contained in the evaluation report. Shortly we will forward information on the corrective actions to be taken regarding these recommendations and the target dates for completion.

Enclosed you will find our Management Reaction comments which we hope to see included in your evaluation report.

Any comments or questions can be directed to our Cyber Security Officer, Steve Novak, at 202-502-6371.

Enclosure
1 - Management Reaction comments

MANAGEMENT REACTION

The Federal Energy Regulatory Commission (FERC) is one of only a handful of small agencies that attempted to comply with GISRA requirements in FY2001. We were commended for our efforts during a meeting with OMB earlier this summer. During that meeting we informed OMB that our major weakness was a lack of documented policies, procedures and guidelines but that we were making progress in laying the foundation for an effective cyber security program. FERC continues to make progress in achieving its cyber security goals and implementing corrective actions to ensure protection of FERC information and information systems. However, being a small agency, FERC does not have the extensive resources needed to implement and execute a fully robust cyber security program in an expeditious manner. However, we acknowledge many of your conclusions and observation and have developed or are in the process of developing plans to achieve cyber security program objectives.

FERC has addressed many of the observation identified in your evaluation report by enhancing certain elements of the cyber-security program, and is planning to incorporate a full suite of documented policies, procedures, and guidance that will provide the framework for a more fully developed cyber-security program.

In FY 2002, FERC focused on strengthening its cyber-security in the areas of management, technical, and operational controls. The capstone document that addresses these areas is the *Cyber Security Action Plan (CSAP)*. The intent of the CSAP is to serve as a strategic roadmap for implementing the components for the FERC cyber security program. While differing with your observation, our strategy was to provide detailed milestone dates in a number of additional cyber security implementation plans which collectively would outline the approach for implementing the FERC cyber-security Agency-wide strategy. These implementation plans will detail next steps for program sub-elements, including IT security compliance, IT security metrics, IT security awareness & training, certification & accreditation, risk management, configuration management, and incident response. These implementation plans will be disseminated throughout FERC using a comprehensive information assurance (IA) communications strategy.

We recognize the need to accomplish many of the actions identified in your observations. Our focus during FY 2002 was to establish the foundation on which to build. In addition to the CSAP, on June 27, 2002, the Chairman released a memorandum to all Office Directors outlining the FERC cyber security program, and addressing the need for increased emphasis on the GISRA review process. The memorandum specifically outlined the following:

- Mandate that the OCIO will lead and coordinate the GISRA activities across the Commission
- Mandate that all Office Directors take a more active role in ensuring adequate security for their systems, as well as appoint an Information System Security Manager (ISSM) to manage each major application
- Direct that the OCIO will provide the necessary training to all Office Directors and ISSMs on GISRA activities

These mandates have subsequently been initiated to include developing and providing GISRA specific training to Office Directors and ISSMs by OCIO in July 2002. Additionally, cyber security self-assessment training was also developed and provided to ISSMs. With this memorandum, we are now positioned to take the next steps in implementing a cyber security program and support structure at FERC.

The CSAP addresses the system security planning and continuity planning observations identified in the

Appendix 3 (continued)

evaluation report. One of the principal components identified is a formal Certification and Accreditation (C&A) process. We completed development of a *C&A Methodology* document that includes the development of system security plans (SSP), and continuity plans. We are in the process of selecting a pilot system to validate the methodology and then we will develop prioritized schedule for completing C&A of all FERC systems.

FERC recognizes the importance of training to the success of a cyber security program. Although not a mandated requirement, we took the initiative to explore the cost-benefit of developing web-based cyber security awareness and training. The initiative was placed on-hold when an announcement of the development of a standard federal government web-based cyber security awareness and training package was underway. Should this not materialize in the near future, FERC will re-explore the web-based cyber security awareness and training option.

FERC has always been aggressive in ensuring proper configuration management and access controls for its systems. Our proactive approach was demonstrated when we initiated an additional requirement to conduct external and internal penetration testing of our systems for the 2002 GISRA review. Although several weaknesses were identified, our network security administrators took immediate action to correct all weaknesses before the completion of the overall evaluation.

In May 2002, we performed a review of the Commission inventory of systems. The purpose of the review was to reconcile differences, if any, between the FY01 GISRA systems inventory and the FERC Applications Names Listing maintained by the Systems Engineering Division. Mission criticality was not considered in the inventory and systems/applications were not categorized as such. However, a cursory review determined that no system qualified as mission critical as defined by Section 3532(b)(2) of GISRA. However, FERC does plans to evaluate the inventory to determine if there are system/applications that are of significantly greater importance to the business processes of the Commission – in short, “business critical” systems.

FERC understands that a managed approach to tracking, calculating, reporting, and analyzing data to evaluate office performance is a critical component to a successful cyber security program. This year, for the first time, FERC will establish a performance baseline using the performance measures as defined in the OMB Memorandum entitled “*Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Actions and Milestones*”. Our plans are to continue to develop, mature and integrate these cyber security metrics into our cyber security program.

Over the course of the next year, FERC will strive to achieve higher levels of compliance with GISRA and *OMB Circular A-130* by working to close audit findings and material weaknesses through corrective action plans. It should be noted that we had already identified, documented, and established completion dates for corrective action for the majority of the observation in the evaluation report in our Plan of Action and Milestones. Ultimately, in FY 2003, FERC plans to begin the C&A process for all major applications and general support systems as the key to reducing vulnerabilities and managing risk, and will work to continually improve our strategy as the path to sustaining its GISRA-compliant cyber-security program.

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit would have been helpful to the reader in understanding this report?
2. What additional information related to findings and recommendations could have been included in this report to assist management in implementing corrective actions?
3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?
4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy, Office of Inspector General, Home Page
<http://www.ig.doe.gov>

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.