

**COMPUTER SECURITY AND CONTROLS
AT THE AIRCRAFT REPAIR AND SUPPLY CENTER**

U. S. Coast Guard

*Report Number: FI-2003-022
Date Issued: February 25, 2003*




Memorandum

**U.S. Department of
Transportation**

Office of the Secretary
of Transportation
Office of Inspector General

Subject: **ACTION:** Report on Computer Security
and Controls at the Aircraft Repair and
Supply Center, U.S. Coast Guard
FI-2003-022

Date: February 25, 2003

From: Alexis M. Stefani 
Principal Assistant Inspector General
for Auditing and Evaluation

Reply to
Attn. of: Meche: x61496

To: Chief of Staff
U.S. Coast Guard

This report provides a summary of the results of the computer security and controls audit at the U.S. Coast Guard (Coast Guard) Aircraft Repair and Supply Center (the Center), Elizabeth City, North Carolina. The audit was conducted by PricewaterhouseCoopers (PwC) LLP under contract with the Office of Inspector General (OIG). The audit objective was to determine whether the Center's computer operations are adequately secured to ensure integrity, confidentiality, and availability of Coast Guard operations in support of the Department of Transportation Fiscal Year (FY) 2002 Consolidated Financial Statements.

We performed a quality assurance review of the PwC audit work to determine compliance with applicable standards. These standards include Government Auditing Standards and the Federal Information Systems Controls Audit Manual published by the Comptroller General of the United States. We assessed PwC staff's independence and qualifications, discussed the project scope and objectives, approved the PwC audit plan, held biweekly status meetings, and reviewed detailed findings before they were presented to the Coast Guard. The audit scope and methodology are discussed in Exhibit A.

The Center performs many functions that support Coast Guard aircraft, including maintenance, engineering technical support, supplies, and information technology services. The Center also houses two Coast Guard systems that track aircraft maintenance, manage inventory for financial statement data, and support aircraft operations. PwC conducted its audit of Coast Guard's computer operations and

provided its reports¹, with detailed findings and recommendations, to the Center's Commanding Officer. The key issues are summarized below.

RESULTS

At the Aircraft Repair and Supply Center, Coast Guard needs to (1) establish a disaster recovery and business continuity plan, (2) strengthen access security to the Center computer systems and physical complex, (3) strengthen the Center's process for controlling changes to production systems, and (4) enhance security administration functions including background checks on key personnel.

Disaster Recovery and Business Continuity Planning

- The Center did not have a disaster recovery or business continuity plan to resume operations timely should the current site become unavailable. The Center computer systems support Coast Guard aircraft that carry out mission-critical functions, such as search and rescue; securing seaports; and law enforcement. If these computer systems become unavailable for an extended period, Coast Guard may have to ground its aircraft.
- The Center's protection of critical backup files needs improvement to ensure recovery of system operations. While backup files were produced on a daily basis, the Center sent the backup files to off-site storage once a month. This practice could result in the loss of up to 30 days of data. On-site storage also was not adequate. The safe used to store backup tapes was not fireproof and was located in an unsecured place without climate control. As a result, there is an increased risk that the backup tapes stored temporarily at the Center would be unusable or inaccessible in the event of a disaster.

Access Security

- Separated employees were not removed as authorized users from the computer system access listings. A review of records of 45 separated employees showed that accounts for 19 of the 45 employees were still in the computer systems. These invalid accounts could be exploited for unauthorized use.

¹ PwC provided two detailed reports--one on access security and the other on disaster recovery and business continuity, system change controls, and security administration. For security reasons, specifics concerning the weaknesses and audit procedures are not discussed in this report, but were provided to Coast Guard managers during the audit.

- The Center network computers had vulnerabilities. These vulnerabilities did not expose computers to intrusions from the Internet; however, they were available for exploitation by personnel working at the Center. For example, by testing on-site within the Center, PwC was able to gain full access to Center computer systems and about 200 individual workstations.
- The card key system used to control and record individuals' access to the building housing the computer systems was not fully activated nor properly maintained. Employees separated from the Center and personnel with temporary access were not removed from the database. Also, the card key system was activated only after regular working hours. As a result, should an event occur during regular working hours, the Center would not be able to identify individuals who entered the building during the day.
- Physical security and fire protection in the Center's computer building were not adequate. Specifically, there were no surveillance cameras or motion detectors in the building. Also, auditors observed that the loading dock door was open after normal work hours and the exterior door to the telecommunications closet was not locked. Fire-resistance walls surrounding the computer center were constructed between dropped ceilings and raised floors, rather than from the concrete floor to the top of the building. As a result, in the event of a fire emergency, fire and smoke could spread easily into the computer center.

System Change Controls

- System development personnel were given full access to production systems, including the capability to modify computer programs and production data. System changes should be made and reviewed in a test environment and only approved changes should be accepted into production systems. To ensure these controls are not bypassed or omitted, system development staff responsible for making program changes should not be given access to production systems.
- Changes to application program codes in the two computer systems were not made consistently according to Center procedures. A review of 45 system changes identified 30 changes where required documentation was missing. For example, the Functional Test Checklists were missing or contained incomplete sign off for 9 of the 30 changes. As a result, there was no evidence that program codes were adequately tested, as required by the Center, before being placed into production systems.

- The Center did not have established procedures for documenting, testing, or approving changes to computer operating systems² in the Center. Without a formally documented operating systems change process, unapproved or untested changes could be installed on production systems.

Security Administration

- Background checks on employees and contractor personnel were not always conducted. A review of 45 individuals identified no documented evidence of background checks for 16 of the 45 individuals, consisting of military, civilian, and contractor personnel. As a result, the Center may have missed valuable information that might keep some at risk personnel from working on Center computer systems.
- Employee confidentiality agreements were not always required and security awareness statements were not located in the records for 6 of the 45 individuals reviewed. Also, only 8 of the 45 authorized system users reviewed had an access authorization form on file that gave them written permission to access the system. The security administrator was not periodically re-certifying users' need to access the Center's systems, nor routinely reviewing system security violation logs.
- Employee termination and transfer policies were not formally documented or enforced. As a result, employee separation checklists were not consistently completed. A review of 45 files showed 25 did not have a separation checklist. Use of the separation checklist ensures timely removal of separated employees from the system access list.

CONCLUSION

In our opinion, the audit work performed by PwC complied with applicable standards. PwC provided detailed recommendations to the Center management. The complete listing is in Exhibit B. Therefore, we are not making any additional recommendations. However, in our opinion, the following are key action items that Coast Guard officials should implement on a priority basis.

1. Develop and periodically test detailed disaster recovery and business continuity plans, deliver the Center's backup tapes for off-site storage more frequently than once per month, and store the tapes on-site in a fireproof safe located in a secure environment with climate control.

² Unlike application program codes, operating systems do not support specific business functions. Instead, they handle housekeeping functions in computers such as apportioning memory space, scheduling tasks, or managing information flow among all devices.

2. Enhance computer systems access security by timely removing access accounts for separated employees; correcting vulnerabilities identified on the computers tested; and assessing whether corrections are needed for other computers.
3. Strengthen physical security and fire protection by activating the access card reader system 24 hours a day; removing separated employees from the system; installing surveillance cameras or motion sensors; securing exterior doors to the building and telecommunications closet; and extending fire-resistance walls surrounding the computer center.
4. Protect production systems by restricting system development staff's access; requiring all development groups to consistently document application program changes; and establishing procedures for processing changes to operating systems software in production systems.
5. Strengthen system security administration functions in the areas of conducting background checks; re-certifying users' need to access Center systems on a periodic basis; timely reviewing security violations log for followup actions; and enforcing use of access request forms, confidentiality agreements, and separation checklists.

MANAGEMENT COMMENTS

On December 31, 2002, PwC provided its detailed findings and recommendations to the Center's Commanding Officer. The Commanding Officer generally concurred with the findings and has initiated corrective actions based on consideration of risks, funding, and policy. He also agreed to provide a written response upon receiving the OIG final report.

OFFICE OF INSPECTOR GENERAL RESPONSE

We request that Coast Guard provide written comments to recommended action items above by February 28, 2003, to include specific action plans and estimated completion dates. Because the Coast Guard is transferring to the Department of Homeland Security (DHS) on March 1, 2003, we will provide this report, along with Coast Guard action plans and estimated completion dates, to the DHS Office of Inspector General for followup to ensure corrective actions are taken.

We appreciate the courtesies and cooperation of Coast Guard and PwC representatives. If you have questions concerning this report, please call me at (202) 366-1992, or John Meche at (202) 366-1496.

EXHIBIT A. SCOPE AND METHODOLOGY

Under contract with the OIG, PwC conducted an audit of computer security and controls for the two information systems housed at the Center. The audit covered FYs 2002 and 2003 activities, and was conducted from October to December 2002.

OIG and PwC met to discuss the project scope and objectives. PwC conducted the review based on an OIG-approved audit plan. PwC then conducted fieldwork in accordance with the plan, including interviews, reviews of documentation, observation of procedures, and testing of control features.

OIG performed a quality assurance review of the PwC audit work to determine compliance with applicable standards. PwC conducted this audit in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States, the General Accounting Office Federal Information System Controls Audit Manual, and supplemental PwC review guides.

EXHIBIT B. PwC RECOMMENDATIONS

Disaster Recovery and Business Continuity Planning

- The Center should develop and test detailed disaster recover and business continuity plans, and establish procedures for re-testing these plans on a regular basis.
- The Center should deliver backup tapes for off-site storage more frequently than once per month, and store the tapes in a fireproof safe located in a secure environment with climate control.

System Access Security

- The Center should implement procedures to ensure that systems security personnel are timely notified of employee transfers or terminations for immediate removal of their user access accounts.
- The Center should automatically suspend inactive user accounts after conversion to a new technical platform. Meanwhile, the Center needs to develop procedures to ensure inactive user accounts are manually suspended after 120 days.
- The Center should restrict system developers' access to the program changes control software so developers could not transfer program changes to production systems. The Center should also periodically re-certify authorized users and eliminate shared user accounts.
- The Center should remove system developers' access to production systems and revise procedures for granting access on an as-needed basis.
- The Center should correct vulnerabilities identified on the computers tested and assess whether corrections are needed for other Center computers. The Center should also consider implementing technical configuration standards by using guidance developed by other Federal agencies. If implemented, the Center needs to provide training to system administrators and develop procedures for enforcement.

Physical Security

- The Center should conduct a formal physical security risk assessment of the facility and strengthen general security at the perimeter guard station. The

Center should also secure the computer center building by activating the physical access card readers all the time, installing surveillance cameras or motion sensors, monitoring the computer center 24 hours a day, locking exterior doors to the building and telecommunications closet, extending fire-resistance walls in the computer center, closing cabinet doors, and removing combustible materials.

- The Center should re-certify users authorized to access the computer room in the card reader system and develop enforcement procedures for granting, re-certifying, and revoking user access and reviewing failed access attempts.

Systems Change Controls

- The Center should uniformly require all development groups to prepare and complete documentation supporting program change management process, including the formal approval of all relevant checklists, test plans, and other change control documents.
- The Center should establish and enforce written procedures for testing and implementing changes to the operating systems software used to support production systems.

Security Administration

- The Center should work with the Coast Guard Chief Information Officer's office to develop, implement, and enforce procedures to update the entity-wide security plan on a regular basis (at least annually), ensuring that the formal approval of executive management is obtained and documented.
- The Center should reconcile inconsistencies in policies regarding background checks, and perform background checks on all Center employees and contractors with access to sensitive information, including any access to the Center's networked systems.
- The Center should require all personnel to sign confidentiality agreements.
- The Center should require all employees to periodically read and sign Security Awareness Statements certifying that they are aware of and understand all security policies, their individual security responsibilities, and the consequences of failing to adhere to the security guidelines.

- The Center should make its security awareness information readily accessible to employees.
- The Center should use its standard system access authorization form on a consistent basis. Additionally, all access requests, including physical access to sensitive areas of the Center and remote access to systems, should be completed using a standard access request form.
- The Center should implement a routine process for periodically reviewing access privileges to ensure that access has been properly assigned and remains properly assigned based on the principle of least privilege required to perform assigned job responsibilities. Additionally, the security manager should review sensitive system access as it is granted to ensure that the resulting access privileges are appropriate.
- The Center should document and enforce formal termination and transfer policies and procedures. These documents should include information related to the return of property, the suspension of user accounts, and the removal of terminated employees from the premises.
- The Center should implement and enforce procedures requiring that the separation checklist be completed during all exit interviews.
- The Center should develop and implement formal procedures for routinely monitoring security violation logs, promptly investigating any questionable activity, and reporting the results to appropriate levels of management.