Office of Inspector General

Audit Report

USMMA SECURITY CONTROLS WERE NOT SUFFICIENT TO PROTECT SENSITIVE DATA FROM UNAUTHORIZED ACCESS

Maritime Administration

Report Number: FI-2012-138
Date Issued: May 30, 2012

Memorandum

U.S. Department of Transportation
Office of the Secretary
of Transportation
Office of Inspector General

Subject: ACTION: USMMA Security Controls Were Not Sufficient to Protect Sensitive Data from Unauthorized Access
Maritime Administration
Report No. FI-2012-138

Date: May 30, 2012

From: Louis C. King
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA–20

To: Maritime Administrator

The United States Merchant Marine Academy (USMMA), located in Kings Point, New York, is the Federal Service Academy—operated by the Department of Transportation's (DOT) Maritime Administration—responsible for training shipboard officers for the U.S. Merchant Marine. It is a fully accredited, degree-granting institution, and as an institute of higher education, USMMA possesses sensitive information, including current and former students' grades and personally identifiable information (PII), such as social security numbers and passport numbers. The Academy uses a local area network (LAN) and Website for several purposes, including the acceptance of student applications and maintenance of student grade records, both of which include PII.

We initiated this audit in response to weaknesses identified at USMMA during the fiscal year 2010 information security audit required by the Federal Information Security Management Act of 2002 (FISMA). Our objectives were to: (1) determine whether USMMA's LAN and Website are secure from compromise; and (2) identify security weaknesses in the Academy's LAN, Website and databases.

To conduct our work, we performed an external penetration test[1] to determine whether unauthorized access to USMMA's Website and network was possible. We also visited USMMA to perform onsite vulnerability assessments that would

[1] A penetration test is a method of computer security evaluation that involves the simulation of a malicious attack on information systems. The objective of the test is to determine whether external and/or internal parties can acquire unauthorized access to the systems.

identify control weaknesses. Finally, we used a statistical sample of USMMA's user systems to evaluate compliance with required configuration baselines. We conducted this audit between February 2011 and March 2012 in accordance with generally accepted Government auditing standards.

RESULTS IN BRIEF

USMMA's security controls were not sufficient to protect its Website and LAN from compromise, as USMMA had not implemented security controls required by National Institute of Standards and Technology's (NIST) guidance and DOT policy. In March 2011, we successfully penetrated USMMA's network security through a misconfigured application on its Web server, and due to excessive account privileges and poor access controls on the LAN, were able to gain full access to the Academy's LAN and sensitive information. Our test demonstrated that all USMMA data, including PII, is at high risk of exposure to hackers. As a result of our work, USMMA corrected the vulnerability in its Web server that allowed our remote penetration during the audit,[2] but did not correct the other weaknesses we found on the LAN.

Additional information security weaknesses exist in USMMA's LAN, Website and databases because the Academy has not implemented information security programs for protection of information and information systems, as required by FISMA and DOT policies. For example, poor access controls over the Academy's databases make its PII vulnerable to unauthorized access. Other security management weaknesses—including missing software update patches;[3] ineffective security management tools; excessive account privileges; unnecessary accounts; insecure system configurations; ineffective contractor oversight; and the use of an internet connection that did not comply with the Trusted Internet Connection (TIC) requirement[4]—put its entire system at risk for compromise. USMMA's management attributed the identified security weaknesses to insufficient resources and contractors' lack of knowledge about Federal information security requirements. As a result, the USMMA runs the risk that intruders will gain unauthorized access to the large amount of sensitive information stored in its system without detection or response from USSMA.

We are making recommendations to assist USMMA in the establishment of an effective information security program.

---

[2] Immediately after we succeeded in the penetration of the network, we notified appropriate officials to address the exploited vulnerability.

[3] A patch is software designed to update or repair a problem, such as a security vulnerability, in a computer program.

[4] Office of Management and Budget's (OMB) M-08-05, "Implementation of Trusted Internet Connections (TIC)," November 20, 2007, requires agencies to consolidate external network connections to improve security and better monitor threats across Federal networks.

BACKGROUND

Because it is an institute of higher education that is also a Federal Executive Branch entity, USMMA faces special challenges in compliance with its regulatory information security requirements. It must follow all Federal and DOT information security policies, per FISMA, as well as the laws and regulations that govern academic records and performance. To meet its missions, USMMA must collect sensitive personal information, including social security numbers, medical histories, family information, and student academic histories from over 1050 current midshipmen,[5] 80 faculty, and support staff, as well as alumni. This large amount of sensitive information results in a significant responsibility for USMMA with regards to the information's security.

The Academy relies on its information systems to handle applications, provide class room services, maintain midshipmen's records, and provide administrative support. It uses a single network to both support its academic mission and handle administrative tasks. The development, operation, and security of all of USMMA's information systems are provided under a single services contract. The contractor provides all information technology (IT) services to the Academy under the direction of its Chief Information Officer (CIO). The contractor also provides IT support to the midshipmen on campus, including the issuance and maintenance of student laptops. The midshipmen take these laptops with them when they serve for required periods at sea, and the Academy must continue to provide IT support during these periods.

OIG GAINED REMOTE ACCESS TO USMMA'S WEBSITE, NETWORK, AND SENSITIVE DATA

We gained total access to USMMA's systems during the March 2011 external penetration test we conducted from DOT's headquarters in Washington, DC. A high-severity vulnerability in USMMA's public Website left the Academy's network completely open to compromise and allowed us to gain access to the Academy's Website, network, and data. A high-severity vulnerability is a weakness that can be used to remotely gain control of a system. Other system weaknesses aided our intrusion, including USMMA's posting of its password policy on its public Website, weaknesses in the Academy's system settings and use of administrative accounts, and poor incident detection. Our test demonstrated that all USMMA data, including PII, was at high risk of exposure to hackers.

[5] As of its Fall 2011 enrollment.

We requested that USMMA provide us with all data (e.g. computer logs) related to our intrusion to determine whether hackers had successfully compromised the system prior to our test. However, the system administrator had deleted the Web server traffic history and was unable to fully recover the data. The partially reconstituted files were not useful for analysis, so we were unable to make this determination. The deletion of the history files was contrary to the Academy's System Security Plan for the LAN, which states that all logs are to be retained for at least one year. As a result, it is unknown whether the flaw in the web server software had been previously exploited and if so, what data had been accessed.

The weaknesses that we exploited were present in USMMA's system because the Academy has not followed NIST's guidance[6] and DOT's policy[7] for protecting information systems. NIST's Special Publication (SP) 800-44 Revision 2 provides guidelines for securing public Web servers—security that would have prevented exploitation of the vulnerability that allowed our access to the network. NIST and DOT also require implementation of standard security controls—which the Academy has not adopted—that include minimum acceptable requirements for configuration management,[8] account management,[9] incident detection and response, and audit log retention. Furthermore, USMMA does not actively monitor the tools that detect possible intrusions such as the one we conducted, and instead reviews the information that the tools provide only after an intrusion is evident.

The Academy has corrected the high-severity vulnerability in its Website that we used to compromise the Web server. However, it has not corrected the other weaknesses we exploited to gain full network access. These weaknesses and those we detected in our on-site vulnerability assessment are discussed below. As a result of these ongoing problems, USMMA remains vulnerable to the loss of PII and would not be prepared to detect or respond to another compromise of its system.

---

[6] NIST SP 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009

[7] DOT Departmental Cybersecurity Compendium, June 14, 2011

[8] A process that ensures that system owners use approved security control baselines for all software. The baselines prescribe the ideal software settings to attain the required degree of security.

[9] A process that creates, modifies and terminates network accounts, including user accounts. System owners use these accounts to grant and control user access.

ADDITIONAL SECURITY WEAKNESSES MAKE USMMA's NETWORK VULNERABLE

Our May 2011 on-site vulnerability assessment revealed many security control weaknesses in USMMA's system. Database security weaknesses make PII vulnerable to unauthorized access. Furthermore, missing software updates, ineffective security management tools, poor account management, weaknesses in the Academy's security configuration management, the use of an unapproved internet connection, and inadequate management participation in security and contractor oversight put the Academy's entire system at risk for compromise.

Weaknesses in USMMA's Database Security Make PII Vulnerable

USMMA's database management systems had configuration and account management vulnerabilities that jeopardize system security. For example, use of midshipmen and other users' PII in application development and testing combined with weak passwords allowed access to PII, including social security numbers, passport numbers, and password reset questions. Furthermore, all nine database systems we discovered during our network inventory had high severity vulnerabilities that can allow unauthorized access to them and to the server they run on. For example, default settings, which provide access to sensitive data and privileged administrator commands, are accessible to users who do not need access to them to perform their work.

The Privacy Act[10] requires appropriate administrative and technical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. DOT's Departmental Cybersecurity Compendium requires each System Owner—the official responsible for the development and operation of a system—to implement a process for privileged account management, and institute least-privilege access. Least privilege means that a user is assigned the minimum rights they need to perform their duties. Because USMMA management gave software developers and database administrators complete control of the Academy's systems and did not conduct security assessments, they were not aware that developers and administrators had not applied the required security controls when they configured the databases. Consequently, PII was easily available to anyone with access to USMMA's network. Furthermore, access to the password reset information allows a hacker to reset another user's password and log on to a system as that user. This unauthorized login would allow the hacker to view the user's email, connect to

[10] 5 U.S.C. § 552(e)(10)

other systems as the user, and access any sensitive data available to the user—all without an audit trail that would lead back to the hacker.

The Academy Does Not Properly Update Its Software Applications' Security Patches

USMMA did not ensure that applications installed on servers and user systems were fully patched. USMMA's system for automatic patch deployment was mostly effective in patching operating system[11] vulnerabilities, but did not properly remediate installed applications. During our vulnerability assessment, we found 250 missing patches for high-severity vulnerabilities across 23 servers and support systems in the management portion of the network, the majority of which were in third-party applications. Third-party applications, such as Adobe Reader or Oracle Java, are programs not developed by Microsoft, the Academy's operating system vendor, and are often more difficult to patch since each vendor implements its own update system. As operating systems have become more secure, exploitation of such vulnerabilities in applications has become the primary means for attacks against the systems. USMMA's patch deployment system is not configured to monitor and update all of its third party software.

DOT Order 1351.37, Cybersecurity Policy (June 14, 2011) requires each component's Information System Security Officer (ISSO) to ensure that cybersecurity notices and advisories are distributed to appropriate personnel, and that vendor-issued security patches are expeditiously installed. USMMA did not have a standardized patch management policy or procedures, or a working vulnerability assessment capability. Because it does not patch high-severity vulnerabilities, USMMA's systems remain at risk for compromise.

The Academy's Security Management Tools Are Ineffective

USMMA has invested a large amount of funds to acquire automated tools to assist its administrators with secure system management and to provide Academy management the data necessary to determine the operating status and weaknesses of information systems. However, the following three tools were not effective because they were not configured to properly identify weaknesses:

- A vulnerability assessment tool used to identify missing patches and misconfigurations;
- A compliance monitoring tool used to verify that systems meet OMB and NIST[12] mandated security levels; and

[11] A set of programs that manages computer hardware resources and provides common services to other programs.

[12] OMB M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, March 22, 2007; NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

- A configuration management tool used to install software updates and enforce secure configuration settings.

USMMA did not properly configure its systems to allow remote management by the vulnerability assessment and compliance monitoring tools, resulting in incomplete information on the network's security status. Furthermore, USMMA set up the configuration management tool to apply patches to some but not all of its systems and applications. These vulnerabilities existed because the Academy's IT contractors did not have sufficient knowledge to successfully configure the tools, were not trained in the tools' use, and did not perform routine reviews of the tools' reports. Consequently, the Academy's ISSO was not aware that the tools were not working properly, and did not notice that the reports indicated that the vulnerability assessment and compliance monitoring tools could not access the systems to perform their functions. Finally, because the vulnerability assessment tool was providing incomplete results, the ISSO did not detect missing patches.

DOT Order 1351.37 requires security managers to validate their components' information system security reporting, and ensure that security tools are used to their fullest capacity. USMMA's ISSO had not received sufficient training on the use or implementation of those tools. The CIO stated that the tools were new at the time of our visit and had not yet been fully implemented. Since USMMA's did not configure its security management tools to fully assess the network, management did not have an accurate representation of the system's risk, and vulnerabilities remained unpatched.

The Academy's Account Management Practices Are Ineffective

The practices that the USMMA's system owners use to manage the Academy's user and system accounts do not ensure the accounts' security. We reviewed a list of 20 accounts and found 16 active service accounts—used to run various software with domain administrator rights. These rights grant full control to a Windows network and allow anyone that gains access to these programs to execute privileged commands. Furthermore, the domain administrator account, which we created during our external exploitation of USMMA's Web server, was deactivated, but had not been removed—a fact that shows that USMMA does not actively manage its privileged accounts.

USMMA also did not properly manage the accounts on its student information database. The database administrator provided us a list of 48 current users that needed access to the student record system. We compared this list to a system-generated report of the active accounts, and identified 261 active users. This discrepancy also indicates that the Academy did not actively manage user accounts to remove accounts that were no longer in use. Inactive accounts often have weak passwords and do not alert users when they are locked out, making

them ideal targets for password guessing that leads to unauthorized access to systems. We also reviewed users who had access to social security numbers stored in the database. The Academy's CIO identified two users who should not have had access rights to social security numbers, but informed us that the rights had not been removed due to the users' resistance. USMMA also did not perform account reviews to determine whether all accounts had appropriate access rights based on users' duties.

NIST SP 800-53 requires that agencies use automated methods for account management and systems to audit account creation, modification, disabling, and termination. Furthermore, SP 800-53 requires that system account users have only the minimum access privileges they need to perform their duties. Weaknesses in the Academy's student record system account management allow inappropriate and excessive access to sensitive student data.

Many tools are available to assist with ongoing account management and review, but USMMA had not implemented an automated method. The Academy's CIO stated the Academy did not have the resources to review them manually or acquire a tool to do so. Consequently, accounts were removed and disabled only intermittently, and a large number of unnecessary accounts remained on the system.

The Academy's Security Settings Do Not Meet Baselines

USMMA has not implemented secure baselines for its systems. Baselines are known secure configuration settings that NIST, industry organizations, and system vendors publish, and are required by DOT Order 1351.37 and NIST SP 800-53 Rev. 3.[13] The Academy's network and database administrators informed us that they do not apply known secure baseline configuration settings for the systems—information that we confirmed with the results of our vulnerability scans. We randomly tested 8,547 out of 125,895 baseline controls[14] and found 3,315 controls required by the Government's common baselines were not present. Based on this, we estimate that 48, 829 controls or 38.8 percent of the 125,895 required controls were not present.[15] Even if baselines had been applied, midshipmen and some Academy personnel had administrative rights to the system, meaning they could modify settings on their laptops and install software. We found known viruses and other unapproved programs running on both midshipmen and staff's systems. USMMA's CIO informed us that midshipmen are allowed to install software on their laptops when they are not connected to the network because they own the

[13] The Office of Management and Budget requires departments to apply the Federal Desktop Core Configuration on Windows XP systems and the US Government Configuration Baseline on Windows 7 systems.

[14] Our original universe was 231,231 controls, but at the time of our testing, only 125,895 controls were available due to the fact that some computers were not active at the time of the test.

[15] Our estimate has a margin of error of +/- 0.1 percentage points at the 90 percent level of confidence.

laptops and spend a considerable amount of time away from campus. However, DOT's policy prohibits connection of personally owned equipment to the Department's information systems. The lack of secure configuration baselines prevents assurance that systems operate in a known secure state.

Furthermore, USMMA does not maintain an accurate inventory of its network devices, which is necessary to know what security settings are needed to secure a system. DOT Order 1351.37 requires System Owners to develop, document, and maintain inventories of information system components that accurately reflect the content of their systems. The Academy also did not have a single inventory document. It provided various documents that contained inventory information, but not a complete and accurate inventory of the entire network. For example, a system inventory produced by Active Directory—a Microsoft technology for managing computers, users, and other resources in a Windows-based network—contained hundreds of systems no longer present on the network. The lack of an accurate inventory of network devices means that the Academy cannot be sure that secure configurations are applied to all its devices.

USMMA Did Not Use a Trusted Internet Connection

USMMA was not using a Department-approved TIC to access the Internet. The Academy currently gains internet access through a local provider rather than through one of the three DOT-approved TICs. Approved TIC providers have been certified as providers of the required level of security and monitoring in compliance with OMB's requirements. DOT's Cybersecurity Compendium requires that components convert to use of approved TICs by February 29, 2012 in order to comply with an OMB and Department of Homeland Security mandate to limit and monitor internet connections to Government systems. USMMA informed us that it had not yet been able to procure an approved TIC with sufficient bandwidth to replace its current connection. Because the Academy does not use a TIC, it will be unable to meet the program goals of securing federal agencies' external network connections, including Internet connections, and improving the government's incident response capability.

Management Roles and Participation in Security Were Inadequately Defined

USMMA's System Security Plan (SSP) for the LAN was incomplete. An SSP outlines roles and responsibilities for a system's protection and contains a listing of the system's security controls. The SSP for the Academy's LAN, prepared by an independent vendor who assessed the system in December 2009, did not identify the System Owner or Information System Security Manager—the official responsible for ensuring a system is operating securely. It also did not assign specific responsibilities for information security to the Academy's authorizing

official—the senior manager that accepts responsibility for the information system's operation—or ISSO. Furthermore, the SSP did not correctly identify the Academy's authorizing official or ISSO.

The ISSO, who is a contractor, had primary responsibility for information security operations, but did not ensure that security functioned as intended. The ISSO submitted incomplete or inaccurate reports on system vulnerabilities, did not deploy system baselines, did not ensure that proper backup procedures existed, and did not perform incident detection. The ISSO also had not received sufficient training on the security tools to use them effectively. Furthermore, management did not perform sufficient oversight of the contractor to ensure that controls operated effectively, that security tools were implemented correctly, that contractor system access privileges were managed, and that contractors with security responsibilities received specialized training.

Finally, management did not enforce the network use policy for its midshipmen. The policy met requirements, but had not been officially released or implemented. The midshipmen were not required to acknowledge the policy and were not held accountable for policy violations. For instance, the CIO provided the Commandant's office, responsible for student discipline, with names of midshipmen who accessed adult Websites[16] over the network, but no disciplinary actions were taken.

DOT's Order 1351.37 requires all components to specify functions for System Owners, Information System Security Managers, ISSOs, and authorizing officials for properly implementing their security programs. Furthermore, the Federal Acquisition Regulations require that services contracts for operations and security include specific goals and metrics for acceptable contractor performance, and that agencies oversee contractors' performance. NIST requires that agencies develop and enforce rules of behavior that dictate what users can and cannot do on a network. USMMA's contract lacked goals and metrics, and USMMA's statement of work did not include sufficient detail for the scope of the services being procured. Consequently, management was unable to hold the contractor to specific performance metrics. Furthermore, USMMA's CIO stated that because the contractors were not familiar with FISMA's information security requirements, they did not comply with the requirements. Consequently, critical security weaknesses across the network were not identified for remediation, activities that threaten information security were not monitored, and USMMA's systems and data were at high risk for compromise.

[16] Websites that contain sexually explicit audio, text or images (of partial or full nudity) that in general could not be considered poetic or artistic.

CONCLUSION

PII is a valuable commodity for hackers. The theft of PII can be costly and detrimental to victims and the organizations entrusted with it. USMMA has invested in expensive security tools. However, because the Academy lacks robust policies and technical expertise to make them effective and protect its systems, serious security vulnerabilities exist throughout the Academy's network. These vulnerabilities are exacerbated by the Academy's ineffective security oversight. Consequently, USMMA's systems remain exposed to unauthorized access which can contribute to the loss of staff and midshipmen's PII and the theft of their identities, as well as compromise the integrity and availability of the LAN, Websites and databases.

RECOMMENDATIONS

We recommend that the MARAD Administrator:

1. Establish policies and procedures for account management, configuration management, incident response continuous monitoring, and security training including appropriate metrics for measuring effectiveness.

2. Select and implement approved baseline configurations for all USMMA operating systems, applications, and web servers, document baseline deviations for risk acceptance, and submit to DOT OCIO for review and approval.

3. Review accounts for all USMMA systems and applications to determine if they are necessary, have appropriate access rights, and meet DOT access control requirements. Remove, disable, or modify all accounts not currently in compliance with DOT requirements.

4. Ensure all service accounts have the least privilege necessary to perform their functions.

5. Fully implement continuous monitoring tools, review and validate results, and apply patches or take corrective actions to mitigate vulnerabilities.

6. Enforce acceptable use policies for all users including appropriate corrective actions for non-compliance.

7. Migrate external Internet connection to a DOT approved TIC.

8. Specify security responsibilities for System Owners, Information System Security Managers, ISSOs, and authorizing officials.

9. Ensure management provides contract oversight in accordance with DOT policies and procedures.

AGENCY COMMENTS AND OIG RESPONSE

We provided MARAD's Administrator with a draft of this report on March 27, 2012, and received its written response on May 1, 2012, which is included in its entirety as an appendix to this report. In its response, MARAD concurred with all of our recommendations and detailed planned and completed actions to address these recommendations.

ACTIONS REQUIRED

We consider MARAD's planned and reported actions and target dates responsive to all our recommendations and consider them resolved but open pending completion and documentation of activities. We appreciate the courtesies and cooperation of MARAD's representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1407.

cc: Marilyn Hetsel, Interim Director of Information Technology, USMMA
Bonnie McLendon, MAR-392
Martin Gertel, M-1

EXHIBIT A. Scope and Methodology

We performed our network security assessment between February 2011 and March 2012, and conducted our work at MARAD's Headquarters in Washington, D.C. as well as USMMA's facility in King's Point, New York. We conducted our audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To address our audit objectives, we used the guidance provided in NIST SP 800-115 Technical Guide to Information Security Testing and Assessment (September 2008) to perform a penetration test and vulnerability assessment of USMMA's LAN and Website using widely available tools and techniques. We interviewed USMMA's CIO, information technology contractors, and senior leadership to determine what information and resources were critical to USMMA's operation and how protections were implemented. We reviewed and analyzed documents, policies, and procedures related to USMMA's network infrastructure and Website.

Finally, we used a statistical sample of 68 of 1,001 computers from USMMA's system inventory to evaluate compliance with required configuration baselines. For the 37 of the 68 that were available at the time of testing, we used a NIST validated configuration assessment tool to compare each computer's operating system settings to the appropriate baseline configuration. We tested 231 controls on each of the 37 computers for a total of 8,547 controls. This statistical sample allowed us to project missing controls with a 90 percent confidence level and a margin of error of 0.1 percentage points for the computers that were available.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Louis C. King	Former Program Director
Gerald Steere	Project Manager
Felicia Moore	Information Technology Specialist
Susan Neill	Writer-Editor
Megha Joshipura	Statistician

APPENDIX. AGENCY COMMENTS

U.S. Department of Transportation
Maritime Administration

Memorandum

Subject: Management Response to OIG Draft Report on USMMA Information Technology Security Controls

Date: May 1, 2012

From: David T. Matsuda
Maritime Administrator

Reply to Attn. of: MAR-340

To: Louis C. King
Assistant Inspector General for Financial and Information Technology Audits

The Maritime Administration (MARAD) and its United States Merchant Marine Academy (USMMA) recognize the critical importance of protecting information technology infrastructure and the personally identifiable information (PII) that it contains. The Office of Inspector General (OIG) team assigned to this report was able to apply the tools and expertise necessary for the types of real-world testing that have proven invaluable in identifying and acting upon vulnerabilities. Over the past year since the testing was completed, MARAD and the USMMA have addressed many of the measures called for in this report; nonetheless, significant challenges remain.

Most of the specific policies called for in the report have been completed, standard operating procedures enumerated and implemented, and network capabilities installed on the system to perform real time monitoring. USMMA has made significant progress in the application of Information Technology Infrastructure Library (ITIL), identifying policies reflecting best practices and recommended baselines, and implementing the necessary procedures, but these endeavors are still a work-in-progress. The primary challenges revolve around resources, both human and budgetary. It is particularly difficult to secure an adequate cadre of skilled individuals to maintain and enhance the security of the network. We are also challenged with the restrictive budgetary environment which will further limit the nature and pace of continued improvement.

Following are responses to the specific recommendations in the report. Due to the nature of the subject matter, some specific aspects of the responses, along with documentation will be provided under separate cover.

Recommendations and Responses

Recommendation 1: Establish policies and procedures for account management, configuration management, incident response, continuous monitoring and security training including appropriate metrics for measuring effectiveness.

Response: Concur. USMMA recognizes that at the time of the OIG testing, documentation of policies and procedures for IT account management were insufficient. Since then, USMMA has substantially completed the documentation necessary as part of the ITIL Roadmap. Documentation of specific actions taken pursuant to this recommendation, along with milestones for specific actions underway is enumerated under separate cover. While most of these policies have been completed, the last few remaining will be completed by June 30, 2012.

Recommendation 2: Select and implement approved baseline configurations for all USMMA operating systems, applications, and web servers, document baseline deviations for risk acceptance, and submit to DOT OCIO for review and approval.

Response: Concur. USMMA will abide by the NIST SP 800-53 controls guidelines, along with the United States Government Configuration Baseline (USGCB) and the DOT Baselines. The Progress Database does not maintain a federally approved baseline through NIST, Center for Internet Security (CIS), or Defense Information Systems Agency (DISA). The USMMA has followed the general guidelines as published in the FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems" and NIST 800-53, "Recommended Security Controls for Federal Information Systems and Organizations." Specifically to NIST 800-53, we have focused our security efforts in the following categories:

a. Access Controls (AC-2, Account Management)
b. Configuration Management (CM-6, Configuration Settings)
c. Contingency Planning (CP-10, Information System Recovery and Reconstitution)
d. System and Communication Protection (SC-2, Application Partitioning)

The above areas specifically relate to information systems that maintain a database application and are directly related to our application security efforts. In addition, USMMA is currently in the process of migrating away from the Progress Student Information System application to a common and approved platform that does maintain federally approved web and SQL approved baselines. The USMMA is scheduled to complete the database review of Progress by September 30, 2012.

Recommendation 3: Review accounts for all USMMA systems and applications to determine if they are necessary, have appropriate access rights, and meet DOT access control requirements. Remove, disable or modify all accounts not currently in compliance with DOT requirements.

Response: Concur. USMMA recognizes that at the time of the OIG testing, access control reviews were insufficient. Since November 2011, two periodic access controls reviews for

Midshipmen have been performed and will continue to be performed on a quarterly basis. Systems are now in place to remove or disable users when notified by human resources or Regimental Operations, per the established deregistration process. While these reviews will continue quarterly, based on those completed to date, we ask that this recommendation be closed.

Recommendation 4: Ensure all service accounts have the least privilege necessary to perform their functions.

Response: Concur. USMMA recognizes that at the time of the OIG review least privilege access was not being effectively managed. Since the OIG review, new documentation defining roles, responsibilities and processes have been developed to effectively manage service accounts, access rights, and privileges. Currently, USMMA is using a Quality Assurance (QA) process review of privileges regarding functions at the system service level including domain accounts and ensuring least privilege and separation of duties. A request for change automatically generates a QA ticket. Processes have been established for enforcing least privilege and USMMA has also recently implemented a compensating control of oversight review to enforce appropriate access. Based on the actions taken, we ask that the recommendation be closed.

Recommendation 5: Fully implement continuous monitoring tools, review and validate results, and apply Patches or take corrective actions to mitigate vulnerabilities.

Response: Concur. USMMA has completed installation of continuous monitoring tools for its systems. The Security team reviews, validates and implements corrective actions to mitigate vulnerabilities detected. Patch deployment is performed monthly (unless a critical patch is released), and aggregates the patches released by Microsoft Security, third party applications not developed by Microsoft, including Adobe, McAfee, Apple, Mozilla, Safari, and Real Player. After patches have been deployed to midshipmen and Staff, the Security and Service desk team monitors compliance. Patch Reports are run on demand until all systems are in compliance. Based on the actions taken, we ask that the recommendation be closed.

Recommendation 6: Enforce acceptable use policies for all users including appropriate corrective actions for non-compliance.

Response: Concur. A tracking system, AARB, was developed that requires all users of the USMMA network to indicate they understand the use policy and will abide by it. All users are required to accept the policy by selecting the appropriate box during logon and recorded to a database. Unless a user accepts the policy they are not allowed access to the USMMA network. The USMMA Rules of Behavior are the Superintendent's Instructions 2002-2007 for Midshipmen, faculty, and staff, and are agreed to with an electronic signature; they are renewed on an annual basis. In addition, system use notification is displayed at login-time to all client workstations on the USMMA network. The Security Incident team uses the CSMC Incident procedure which follows NIST 800-61 Federal reporting guidelines and timeframes. USMMA maintains an accurate inventory of all network devices and submits monthly Technical

Reference Model updates to MARAD. Based on the actions taken, we ask that this recommendation be closed.

Recommendation 7: Migrate external Internet connection to a DOT approved TIC.

Response: Concur. The Maritime Administration CIO had escalated the unmet need for a TIC at the Academy to the attention of the DOT OCIO. There is no TIC Provider in the area of the Academy and there is a lack of fiber cable in the area so there is no way of obtaining a circuit with sufficient capacity to handle the traffic generated by the Academy. As of this date, the Maritime Administration continues to work with the DOT CIO to identify a cost effective, implementable solution. Our target date for implementation is the end of the second quarter fiscal year 2013.

Recommendation 8: Specify security responsibilities for System Owners, Information System Security Managers, ISSOs and authorizing officials.

Response: Concur. The Policies and Procedures for Roles and Responsibilities have been completed. The roles and responsibilities will become part of the updated System Security Plan, currently under review and is scheduled for completion by July 31, 2012.

Recommendation 9: Ensure management provides contract oversight in accordance with DOT policies and procedures.

Response: USMMA and its contractor now have weekly Security meetings. The agenda includes discussion of the full range of information security issues. The weekly Infrastructure meetings involve a discussion review of all active projects in regard to Network Infrastructure and Applications Operations and Maintenance (O&M). The status of each project is discussed and where necessary plans are revised. Personnel in attendance at these meetings include the MARAD CIO, MARAD contracting officer (CO), ISSM, USMMA interim IT Director, and contractor personnel.

The ISSO identified in the report is no longer with the contractor. There is a new ISSO and three additional security team members who were added to address the findings in this report. USMMA has developed Policies and Procedures for Roles and Responsibilities for functions performed by contractor personnel and are verified as part of the user access control reviews. USMMA also adheres to the NIST guidelines and standards for implementation of technologies in use, as verified by the change management documentation, which is reviewed on a case-by-case basis. Best Practices in all other areas are dictated by MARAD and DOT in order to meet contract requirements.

In July 2011, Academy CIO, CO, MARAD CIO and the contractor executives reviewed USMMA staffing, Performance Work statement and ITIL Road Map. This meeting resulted in mutually agreed program goals and metrics. In February 2012, USMMA's contractor held a Quality Program Review with the Academy CIO and Academy Assistant Superintendent for Plans Assessment and Public Affairs. Three additional security staff have been hired who have

working experience with FISMA and NIST. Based on the actions taken, USMMA believes it has fulfilled the intent of this recommendation and asks that it be closed.

The Maritime Administration would like to thank the OIG audit team for their work in helping the USMMA better secure the IT environment at the Academy. If you have any questions or require additional information, please contact Bob Ellington on extension 6-2531.

cc: Dr. Shashi Kumar, Interim Superintendent
CAPT Eric Wallischeck, USMS, Chief of Staff
Ms. Marilyn Hetsel, Interim Director of Information Technology, USMMA

Appendix. Agency Comments