OFFICE OF INSPECTOR GENERAL
FISCAL YEAR 2018 MANAGEMENT CHALLENGE

FEDERAL MARITIME COMMISSION
Washington, DC 20573
October 12, 2018

Office of Inspector General

TO: Acting Chairman Khouri
Commissioner Dye

FROM: Inspector General

SUBJECT: Inspector General's Statement on the Federal Maritime Commission's Management and Performance Challenge

The Reports Consolidation Act of 2000 (Public Law 106-531) requires inspectors general to provide a summary and assessment of the most serious management and performance challenges facing Federal agencies, and their progress in addressing these challenges. The attached document responds to the requirements and provides the annual statement to be included in the Federal Maritime Commission's (FMC) Performance and Accountability Report (PAR) for fiscal year (FY) 2018.

This year, the Office of Inspector General (OIG) has identified one management and performance challenge, ***information technology (IT) security***. The Commission has continued to make progress on this challenge since last year; IT security remains a government-wide challenge and the FMC's continued focus is critical to ensure an effective security program. This assessment is based on information derived from a combination of sources, including OIG evaluation work; Commission reports; Federal government reports; and a general knowledge of the Commission's programs.

The Reports Consolidation Act of 2000 permits agency comment on the inspector general's statements. Agency comments, if applicable, are to be included in the final version of the FMC PAR that is due by November 15, 2018.

/s/
Jon Hatfield

Attachment

Cc: Karen V. Gregory, Managing Director
Peter J. King, Deputy Managing Director
Kathie L. Keys, Special Assistant to the Managing Director

Office of Inspector General (OIG)
Fiscal Year 2018 Management Challenge

The Management Challenge - Information Technology Security

Information technology (IT) security continues to be a key risk in the Federal government, and as is the case for most Federal agencies, the Federal Maritime Commission (FMC) shares this challenge. While the OIG has found the FMC to be focused on maintaining an effective IT security program, IT security continues to evolve based on new risks and threats. In a report[1] dated September 28, 2017, the Government Accountability Office (GAO) points out that as computer technology has advanced, Federal agencies have become dependent on computerized information and electronic data to carry out operations and to process, maintain, and report essential information. Further, GAO acknowledges that agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Therefore, securing these systems and data is critical.

The GAO maintains a high-risk program to focus attention on government operations that GAO identifies as high-risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges. GAO first designated Federal information security as a government-wide high-risk area over 20 years ago. In 2003, GAO expanded this area to include computerized systems supporting the nation's critical infrastructure and, in 2015, GAO further expanded this area to include protecting the privacy of personally identifiable information. GAO continues to identify Federal information security as a government-wide high-risk area in their February 2017 high-risk update report.

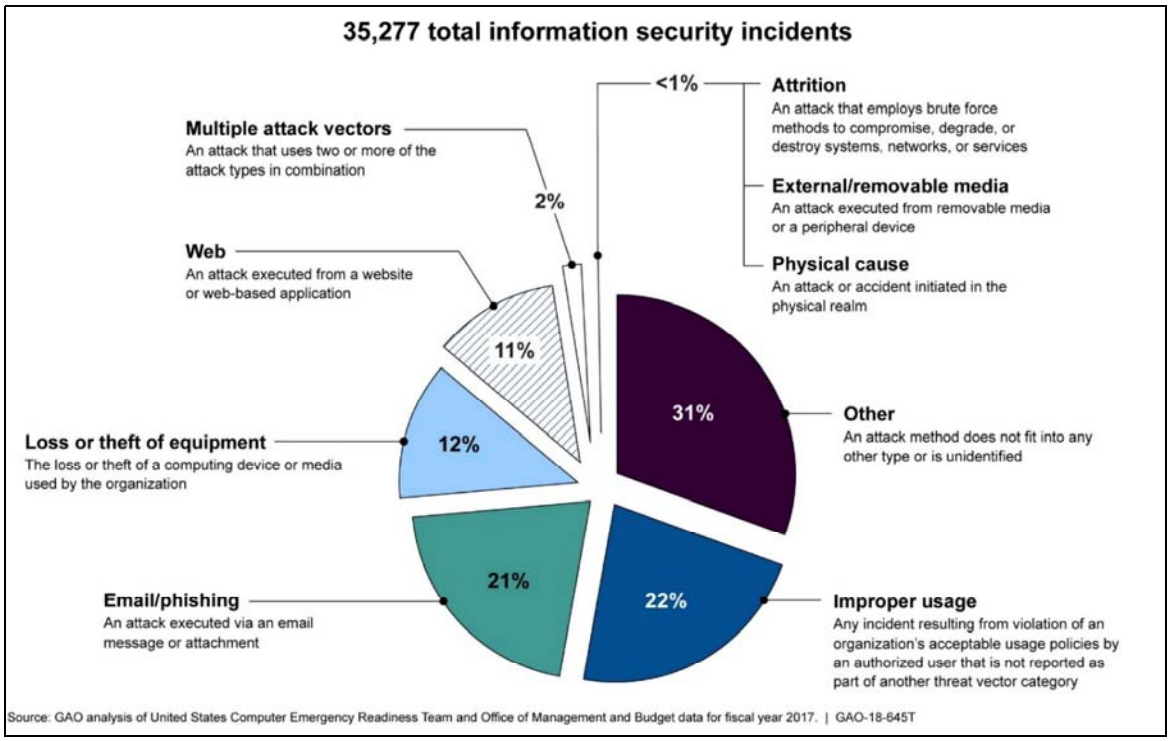
The Office of Management and Budget's (OMB) 2018 Annual Report to Congress on the Federal Information Security Modernization Act of 2014 (FISMA) provides details for fiscal year (FY) 2017 on both the progress and the challenges the Federal government faces to protect computer information systems and data. Specifically, the report states that the President has made strengthening the Nation's cybersecurity a priority from the outset of the administration. For example, among other policies and guidelines, the President issued executive orders in 2017 and 2018 to promote the secure and efficient use of information technology, and reinforcing the FISMA by holding agency heads accountable for managing cybersecurity risks.

OMB's 2018 annual FISMA report to Congress also provides information on the number of cybersecurity incidents that were reported across the Federal government in FY 2017. The

[1] Government Accountability Office, GAO-17-549, Federal Information Security, *Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, (September 28, 2017).

OMB reports that 35,277 incidents were reported[1] by agencies in FY 2017, a 14% increase from FY 2016, as detailed on the following page in figure 1. The report states that e-mail/phishing continues to be a highly-targeted attack, with a 122% increase in reported incidents from FY 2016 to 2017. Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information.

Figure 1: Federal Information Security Incidents by Threat Vector[2] Category, Fiscal Year 2017



Agency Progress in Addressing the Challenge

The *Federal Information Security Modernization Act of 2014* (FISMA) establishes information security program and evaluation requirements for Federal agencies in the executive branch, including the FMC. Each year, the FMC OIG performs an independent evaluation of the information security program and practices of the agency. The results of the evaluation are reported

[1] US-CERT, a branch of the Department of Homeland Security's National Cybersecurity and Communications Integration Center, is a central Federal information security incident center that compiles and analyzes information about incidents that threaten information security. Federal agencies are required to report such incidents to US-CERT.

[2] A threat vector (or avenue of attack) specifies the conduit or means used by the source or attacker to initiate a cyberattack. US-CERT's Federal Incident Notification Guidelines specify nine potential attack vectors agencies should use to describe incident security incidents during reporting.

annually to the Office of Management and Budget; selected congressional committees; the Comptroller General; and the FMC's Commission and management.

In the OIG's *Evaluation of the FMC's Compliance with the Federal Information Security Modernization Act (FISMA) FY 2017*, the OIG found the FMC had effectively implemented all six of the prior year FISMA recommendations. Further, the FY 2017 FISMA evaluation contained two new recommendations to address two findings. The two recommendations involved the timely disabling of computer accounts for separated users, and proper physical controls for the agency's computer server room.

The Challenge Ahead

Significant cybersecurity incidents in recent years highlight that continued advancements in computer and communication technologies will likely result in ongoing challenges protecting Federal systems, to include the FMC. Particularly because of the FMC's small size and limited resources, it is critical for the FMC to prioritize security controls and enhancements based on risk, and continue to properly plan and partner with Federal agencies to protect vital agency resources.

COMMENTS ON INSPECTOR GENERAL-IDENTIFIED MANAGEMENT

The Commission appreciates the Inspector General's essential role in keeping up-to-date on the significant risks and challenges facing the Federal government as a whole, and in reviewing the Commission's work to ensure that it maintains accountability and compliance with Federal laws and mandates. The Inspector General's Management and Performance Challenge – information technology security – poses a significant risk in today's Federal government. A response to the challenge is outlined below:

1. Information Technology Security

   The Commission is aware of the increasing number and sophistication of cybersecurity incidents and threats government-wide, and appreciates working proactively with the Office of the Inspector General to strengthen the Commission's security posture. Protecting our information and information systems against cybersecurity threats and unauthorized access remains a priority at the Commission. Numerous steps have been taken at the Commission to combat the ever-present cybersecurity risk faced by most federal agencies such as viruses, malware, intrusion, and compromised credentials, among other things.

   The FMC has moved to a Managed Trusted Internet Protocol Services (MTIPS) certified internet service provider to comply with the Trusted Internet Connection (TIC) initiative, an OMB mandate. This reduces the number of Internet gateways on the Commission's network and ensures that all external connections are routed through a government agency designated as an approved TIC Access Provider.

   The FMC has moved all email services to Microsoft 365, which provides built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and helps to protect the Commission's network from spam and other malicious files transferred through email.

The FMC is compliant with DHS BOD 18-01, *Trustworthy Email Cyber Hygiene Assessment,* created by the National Cybersecurity Assessments and Technical Services (NCATS) team in DHS National Cybersecurity and Communications Integration Center (NCCIC). This directive's requirements increase the security of emails in transit and make it easier to detect emails that attempt to spoof .gov domains.

The FMC also employs several other types of software which continuously monitor the network looking for the tell-tale signs of virus/malware activity.

To supplement this technology, the FMC provides yearly Security Awareness Training to educate FMC staff and contractors about the different tactics and methods intruders can use to attempt to infiltrate the agency's network. Well-educated FMC staff and contractors are essential to create a culture of accountability and awareness to mitigate risk.

The Commission will continue to focus on this high-risk challenge with careful planning, by making the best use of available resources, and prioritizing our IT security controls.