OFFICE OF INSPECTOR GENERAL
FISCAL YEAR 2017 MANAGEMENT CHALLENGE

FEDERAL MARITIME COMMISSION
Washington, DC 20573

October 12, 2017

Office of Inspector General

TO: Acting Chairman Khouri
Commissioner Dye
Commissioner Doyle
Commissioner Maffei

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) 2017.

The Office of Inspector General (OIG) has identified one management and performance challenge this year, ***information technology (IT) security***. Although the Commission has made progress on this challenge since last year, the OIG acknowledges that IT security remains a government-wide challenge and the FMC will need to remain vigilant to protect the information and information systems of the agency. 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, 2017.

/s/
Jon Hatfield

Attachment
Cc: Karen V. Gregory, Managing Director
Peter J. King, Deputy Managing Director

Office of Inspector General
Fiscal Year 2017 Management Challenge

1. *The Management Challenge* - Information Technology Security

The Office of Inspector General (OIG) recognizes the Federal Maritime Commission (FMC) has continued to make improvements on the agency's information technology (IT) security. Notwithstanding these improvements, the OIG has identified IT security as a management challenge because IT security remains a government-wide challenge and the FMC will need to remain vigilant to protect the information and information systems of the agency.

In a report[1] dated September 28, 2017, the Government Accountability Office 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. As a result, securing these systems and data is critical.

GAO first designated Federal information security as a government-wide high-risk area 20 years ago in 1997. 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 FMC shares with other Federal government departments and agencies this challenge due to the evolving and growing threats to government information systems. Risks to information and communication systems include insider threats from disaffected or careless employees and business partners; escalating and emerging threats from around the globe; the ease of obtaining and using hacking tools; the steady advance in the sophistication of attack technology; and the emergence of new and more destructive attacks.

One of the most recent examples of the challenges faced by Federal agencies to protect information and information systems is the cybersecurity incident at the Securities and Exchange Commission (SEC). In August 2017, the SEC learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading. Specifically, a software vulnerability in a component of the SEC's EDGAR database was exploited and resulted in access to nonpublic information. Another example, first reported in early 2015 by the Office of Personnel Management (OPM), involved the discovery of malicious cyber activity on its network. Two separate but related OPM cybersecurity incidents impacted the data of Federal government employees, contractors, and others. OPM first discovered malicious cyber activity on its network resulting in the exposure of the personnel data of approximately 4.2 million current and former Federal government employees. OPM later discovered malicious cyber activity on its network resulting in the exposure of the background investigation records of approximately 21.5 million individuals, primarily current, former, and prospective Federal employees and contractors. The frequency and increased sophistication of cyber

[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).

threats underscores the need to properly manage and bolster the security of Federal information systems, and to remain vigilant.

Agency Progress in Addressing the Challenge

The *Federal Information Security Management Act of 2002* (FISMA) established 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 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 Management Act (FISMA) FY 2016*, the OIG found the FMC had effectively implemented six of the nine outstanding prior year FISMA recommendations. Further, the FY 2016 FISMA evaluation contained three new recommendations to address three findings; however, two of the three recommendations were implemented by the agency prior to the release of the November 2016 report.

The Challenge Ahead

Significant cybersecurity incidents at Federal agencies, and GAO's continued identification of Federal information security as a government-wide high-risk area, are important reminders that the FMC must continue their focus on protecting the agency's information and information systems.

COMMENTS ON INSPECTOR GENERAL-IDENTIFIED MANAGEMENT AND

The Commission agrees with the Inspector General on the Management and Performance Challenge identified, and remains committed to focusing on this high-risk challenge with careful planning, attention, and diligence. The role of the Inspector General is essential government-wide to ensure government accountability to the American public, and the FMC appreciates its Inspector General's efforts in reviewing the agency's work as well as its compliance with Federal laws and mandates. A response to the challenge is outlined below:

1. Information Technology Security

   The Commission remains ever mindful of the increasing frequency and sophistication of cyber threats, and appreciates working proactively with the Inspector General and his auditor to strengthen the Commission's security posture, and focus on protecting its information and information systems. The cybersecurity incidents mentioned underscore the continuing need for the Federal government to be increasingly vigilant and to constantly monitor, manage, and bolster security controls over Federal information systems. Protecting against unauthorized access to the Commission's information and information systems, and guarding against improper use of computing resources, will remain a priority during the coming years.