INSPECTOR GENERAL'S STATEMENT ON PRIOR MANAGEMENT AND PERFORMANCE CHALLENGES

FEDERAL MARITIME COMMISSION
Washington, DC 20573

October 18, 2019

Office of Inspector General

TO: Chairman Khouri
Commissioner Dye
Commissioner Maffei
Commissioner Sola

FROM: Inspector General

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

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) 2019.

This year's Office of Inspector General (OIG) report removes information technology (IT) security as a management challenge due to the OIG's FY 2019 audit results of the FMC's IT security program, and continued progress by the agency to ensure an effective IT security program. In addition, this report provides an update on the agency's continued focus and positive results on workforce satisfaction and engagement, an issue the OIG no longer considers a challenge for the agency, but was a management challenge during FYs 2013-2015.

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 19, 2019.

/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 2019 Management Challenge Report

Information Technology Security – Prior Years' Challenge

This year, the ***OIG has removed information technology (IT) security as an agency management challenge*** based on the OIG's fiscal year (FY) 2019 audit results of the agency's IT security, and because of continued agency progress over the last several years in this area. The OIG has reported IT security as an FMC management challenge for the last several years primarily because IT security has remained a government-wide challenge due to the evolving and growing threats to government information systems. While the government-wide IT security challenge continues to exist, due to improvements in the FMC's program, the OIG has removed IT security as an FMC management challenge for FY 2019. 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.

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 audit or evaluation of the information security program and practices of the agency. The results of the evaluation are reported annually to the OMB; selected congressional committees; the Comptroller General; and the FMC's Commission and management.

To highlight the importance of IT security, the Government Accountability Office (GAO) has designated information security as a government-wide high-risk area since 1997. This high-risk area was expanded in 2003 to include the protection of critical cyber infrastructure and, in 2015, to include protecting the privacy of personally identifiable information (PII). In addition to GAO reporting, the Office of Management and Budget's (OMB) FISMA FY 2018 Annual Report to Congress highlights the cybersecurity threats facing the Federal government and the need for vigilance to protect the country's data and digital infrastructure. Specifically, Federal agencies reported 31,107 cybersecurity incidents in FY 2018; this is a 12% decrease over the 35,277 incidents that agencies reported in FY 2017.

The OIG plans to issue the final FY 2019 FISMA audit report by October 31, 2019. The anticipated results of the OIG audit are to include three new audit findings and three corresponding recommendations; of the three findings, one was remediated by the end of the FY and is now considered closed. In addition, the final OIG audit report is expected to conclude that all six of the outstanding recommendations from prior years have been implemented by the agency and will be closed. The FMC is demonstrating a commitment to maintain an effective information security program, and the FY 2019 FISMA audit results demonstrate this commitment. The OIG looks for the agency to continue their focus on maintaining and enhancing security controls based on risk and evolving threats.