March 1, 2013

MEMORANDUM FOR: Simon Szykman
Chief Information Officer

FROM: Allen Crawley
Assistant Inspector General for Systems Acquisition
and IT Security

SUBJECT: Audit of Department's Incident Detection
and Response Capabilities

As part of our fiscal year (FY) 2013 Federal Information Security Management Act of 2002 (FISMA) review, OIG is initiating an audit of the Department and its bureaus' incident detection and response capabilities. Our objective is to determine whether key security measures are in place to adequately monitor networks, detect malicious activities, and handle cyber incidents.

Government agencies, Internet commerce, and vital business sectors are all affected by the rapid increase of cyberattacks. In recent years, several Department bureaus have fallen victim to significant cyber intrusions, which allowed attackers to gain unauthorized access to Department systems and information. In order to protect its systems and information, the Department must have a well-established capability to detect malicious network activities in a timely manner and effectively respond to a cyber incident when it occurs.

We plan to immediately survey all Departmental bureaus about their incident detection and response capabilities. Based on survey results, we will select bureaus for our audit and contact their audit liaisons to set up entrance conferences. We will conduct our field work at selected Department and contractor sites.

If you have any questions, please call me at (202) 482-1855 or Dr. Ping Sun at (202) 482-6121.

cc: Brian Callahan, Chief Information Officer, Bureau of Economic Analysis
Eddie Donnell, Acting Chief Information Officer, Bureau of Industry and Security
Brian McGrath, Chief Information Officer, United States Census Bureau
Chuck Benjamin, Chief Information Officer, Economic Development Administration
Renee Macklin, Chief Information Officer, International Trade Administration
Del Brockett, Chief Information Officer, National Institute of Standards and Technology
Joseph Klimavicz, Chief Information Officer, National Oceanic and Atmospheric
 Administration
Daniel Drew, Chief Information Officer, National Telecommunications and Information
 Administration
Keith Sinner, Chief Information Officer, National Technical Information Service

John B. Owens II, Chief Information Officer, United States Patent and Trademark Office
Rod Turk, Director, Office of Cyber Security, and Chief Information Security Officer
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer