Report In Brief

JUN E 26, 2013

Background

The Economic Development Administration's (EDA's) mission is to lead the federal economic development agenda by promoting innovation and competitiveness, thus preparing American regions for growth and success in the worldwide economy. To fulfill its mission, EDA uses six regional offices to provide services specific to each region's needs.

In accordance with the Federal Information Security Management Act of 2002 (FISMA), we evaluated EDA's incident response and recovery activities in relation to EDA's fiscal year 2012 cyber incident.

Why We Did This Review

On December 6, 2011, the Department of Homeland Security (DHS) notified the Department of Commerce that it detected a potential malware infection within the Department's systems. The Department determined the infected components resided within IT systems operating on the Herbert C. Hoover Building (HCHB) network and informed EDA and another agency of a potential infection in their IT systems.

On January 24, 2012—believing it had a widespread malware infection—EDA requested the Department isolate its IT systems from the HCHB network. This action resulted in the termination of EDA's operational capabilities for enterprise e-mail and Web site access, as well as regional office access to database applications and information residing on servers connected to the HCHB network.

Given the Department's limited incident response capabilities and the perceived extent of the malware infection, the Department and EDA decided to augment the Department's incident response team. Additional incident response support was provided by DHS, the Department of Energy, the National Institute of Standards and Technology, and the National Security Agency, as well as a cybersecurity contractor. In early February 2012, EDA entered into an agreement with the Census Bureau to provide an interim e-mail capability, Internet access to EDA staff, and Census Bureau surplus laptops for EDA staff.

ECONOMIC DEVELOPMENT ADMINISTRATION

Malware Infections on EDA's Systems Were Overstated and the Disruption of IT Operations Was Unwarranted

OIG-13-027-A

WHAT WE FOUND

Reviewing EDA's IT security program and the events surrounding its December 2011 c incident and recovery efforts, we found that:

EDA Based Its Critical Cyber-Incident Response Decisions on Inaccurate Information (a) the incident resulted in a widespread malware infection possibly propagating wit systems and (b) its widespread malware infection could spread to other bureaus if it systems remained connected to the network, EDA decided to isolate its IT systems f the HCHB network and destroy IT components to ensure that a potential infection co not persist. However, OIG found neither evidence of a widespread malware infection support for EDA's decision to isolate its IT systems from the HCHB network.

Deficiencies in the Department's Incident Response Program Impeded EDA's Inciden These deficiencies significantly contributed to EDA's inaccurate belief that it experie widespread malware infection. Consequently, the Department of Commerce Compu Incident Response Team (DOC CIRT) and EDA propagated inaccurate information tha went unidentified for months after EDA's incident. We found that DOC CIRT's inciden handlers did not follow the Department's incident response procedures, that its han EDA's incident did not have the requisite experience or qualifications, and that DOC did not adequately coordinate incident response activities.

Misdirected Efforts Hindered EDA's IT System Recovery. With its incorrect interpreta recovery recommendations, EDA focused its recovery efforts on replacing its IT infrastructure and redesigning its business applications. EDA should have concentra resources on quickly and fully recovering its IT systems (e.g., critical business applic ensure its operational capabilities. Our review of EDA's recovery activities found tha (a) EDA decided to replace its entire IT infrastructure based on its incorrect interpret of recovery recommendations and (b) EDA's recovery efforts were unnecessary.

The Department, using already existing shared IT services, returned EDA's systems to former operational capabilities (except for access to another Departmental agency's f system) in just over 5 weeks of starting its effort.

WHAT WE RECOMMEND

We recommend that the Deputy Assistant Secretary for EDA:

1. Identify EDA's areas of IT responsibility and ensure the implementation of requir security measures.
2. Determine whether EDA can reduce its IT budget and staff expenditures, throug increased efficiencies of EDA's involvement in the Department's shared services
3. Ensure that EDA does not destroy additional IT inventory that was taken out of s as a result of this cyber incident.

We recommend that the Department's Chief Information Officer:

1. Ensure DOC CIRT can appropriately and effectively respond to future cyber incid
2. Ensure incident response procedures clearly define DOC CIRT as the incident res coordinator for the bureaus relying on DOC CIRT's incident response services.
3. Ensure that DOC CIRT management has proper oversight and involvement in cy incidents to ensure that required incident response activities take place.