Review of NASA’s Computer Security Incident Detection and Handling Capability (IG-12-017, August 7, 2012)

The NASA Office of Inspector General (OIG) conducted an audit to evaluate the effectiveness with which NASA’s Security Operations Center (SOC) manages the Agency’s computer security incident detection and handling program to prevent unauthorized cyber intrusions into Agency networks.

NASA consolidated its previously Center-based computer security incident detection and response programs into the SOC in November 2008 in an effort to improve its capability to detect and respond to evolving threats posed by increasingly sophisticated cyber attacks. The SOC is intended to provide a single, Agency-wide computer security incident handling capability. Located at Ames Research Center, the SOC provides centralized, continuous monitoring of computer network traffic entering and leaving NASA Centers and includes an information system (the Incident Management System) for Agency-wide coordination, tracking, and reporting of information technology (IT) security incidents.

In general, we found that the SOC has improved NASA’s computer security incident handling capability by providing continuous incident detection coverage for all NASA Centers. In addition, the SOC’s communication processes, including weekly conference calls and security bulletins, were effective for sharing security incident and threat information with responders across the Agency. NASA has also implemented an effective information system that enables Agency-wide management and reporting of IT security incidents.

However, we also found that the SOC does not currently monitor all of NASA’s computer networks. Even though networks we reviewed had their own incident management program that included network monitoring, dedicated staff to respond to incidents and documented processes the networks’ management programs do not provide the centralized continuous monitoring coverage afforded by the SOC. In addition, NASA needs to increase its readiness to combat sophisticated but increasingly common forms of cyber attack known as Advanced Persistent Threats (APTs). APTs are typically designed to bypass the target’s firewalls, intrusion detection system, and other perimeter defenses and are launched by well-organized and well-funded individuals or entities. Moreover, even after the target organization addresses the vulnerability that permitted the attack to succeed, the attacker may covertly maintain a foothold inside the target’s system for future exploits. The increasing frequency of APTs heightens the risk that key Agency networks may be breached and sensitive data stolen.

To enhance NASA’s capability to detect and prevent sophisticated cyber attacks and improve overall SOC availability, the OIG report made three recommendations to the Chief Information Officer. She concurred with our recommendations and proposed corrective actions that that we consider responsive.

THE FULL VERSION OF THIS REPORT INCLUDES MATERIAL NASA CONSIDERS SENSITIVE BUT UNCLASSIFIED INFORMATION WHICH, IF DISTRIBUTED WIDELY, COULD POSE A SECURITY THREAT TO NASA COMPUTER SYSTEMS