Audit of NARA's Web Hosting Environment
OIG Audit Report No. 16-01

NOTE: This is a summary of the complete audit report. The Inspector General has determined publically releasing the complete audit report would unacceptably increase the risk to the agency's information technology systems by disclosing too much information on persistent security deficiencies.

The National Archives and Records Administration's (NARA's) core mission is to provide public access to Federal records. The first goal of NARA's 2014 Strategic Plan, "Make Access Happen," states its objective is to "make all records available to the public in digital form to ensure that anyone can explore, discover, and learn from NARA holdings." However, this cannot adequately happen without NARA's website infrastructure, including NARA's public facing websites and the environments hosting them. Web hosting is the service of providing infrastructure (i.e. web servers and internet connectivity) to publish websites to the internet. According to National Institute of Standards and Technology Special Publication (NIST SP) 800-44, "web servers are often the most targeted and attacked hosts on organization networks." That is why securing the web hosting environment is critical to ensuring the security and accessibility of NARA's Network. This audit of NARA's Web Hosting Environment, included in the Office of Inspector General's Annual Audit Plan, was also requested by NARA's Chief Information Officer.

The objective of this audit was to determine if NARA maintains a secure web hosting environment. Our audit found NARA did not provide consistent oversight and management of the agency's public facing websites and web hosting environments. Therefore, NARA entities were able to create websites without management's approval or knowledge, resulting in an inventory of websites and web hosting environments with greater susceptibility to security and legal vulnerabilities. By not knowing how many websites are managed by NARA entities, its vendors, or partners or where those websites are hosted, NARA has reduced assurance whether all of the public facing websites the agency is responsible for are actually secure.

Further, the Office of Innovation did not classify or categorize NARA's internal web hosting environment in accordance with federal information security standards. These processes are necessary for developing and implementing appropriate security controls. We also found numerous control weaknesses within NARA's internal web hosting environment. As a result, NARA cannot ensure information security protections are in place commensurate with the risk to the confidentiality, integrity, and availability of NARA's internal web hosting environment. In addition, NARA did not require external vendors or partners to conduct and provide security assessments of the systems hosting NARA's websites. As a result, NARA's ability to ensure the agency's external web hosting environments are adequately secure and compliant with federal security standards is severely inhibited, and NARA loses the ability to adequately control and secure IT information hosted on the websites. Should these websites be compromised NARA has no insight or ability to fix them.

This report makes, and NARA concurred with, 33 recommendations to improve NARA's web hosting security and management.