Final Assessment Report 08-01, November 1, 2007, "GPO Network Vulnerability Assessment"

The GPO Office of Inspector General (OIG) completed a vulnerability assessment of the GPO enterprise network infrastructure to evaluate the level of security controls in place that help protect the Agency's information technology (IT) resources from unauthorized access and compromise. We conducted our assessment using vulnerability scanning tools the OIG selected and the GPO Information Technology and Systems Security Division approved. We limited our assessment to the area between GPO's Internet service provider and the outermost firewall interface where GPO's publicly available network resources, such as GPO Access, are hosted. That area is commonly referred to as the demilitarized zone, or DMZ. Our specific assessment objectives were to determine whether GPO:

- Maintained a robust and effective vulnerability scanning and management program that identified and circumvented common internal and external threats to its network.

- Used passwords in the DMZ strong enough to prevent brute force attacks.

- Patched systems in the DMZ in a timely and effective manner.

The OIG issued a sensitive report that found room for improvement and made recommendations to help strengthen security of the publicly available network resources at GPO, but also reduce the risk of system compromise and loss of availability. GPO management concurred with each of the report's recommendations and has initiated responsive corrective actions.