continued efforts needed to address significant weaknesses at IRS

What GAO Found

IRS has continued to make progress in correcting previously reported information security weaknesses. It has corrected or mitigated 49 of the 115 weaknesses that GAO reported as unresolved during its last audit. For example, the agency

- implemented controls for unauthenticated network access and user IDs on the mainframe,
- encrypted sensitive data going across its network,
- improved the patching of critical vulnerabilities, and
- updated contingency plans to document critical business processes.

However, most of the previously identified weaknesses remain unresolved. For example, IRS continues to, among other things, allow sensitive information, including IDs and passwords for mission-critical applications, to be readily available to any user on its internal network, and grant excessive access to individuals who do not need it. According to IRS officials, they are continuing to address the uncorrected weaknesses and, subsequent to GAO site visits, had completed additional corrective actions.

Despite IRS’s progress, information security control weaknesses continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information. IRS did not consistently implement controls that were intended to prevent, limit, and detect unauthorized access to its systems and information. For example, IRS did not always

- enforce strong password management for properly identifying and authenticating users;
- authorize user access, including access to personally identifiable information, to permit only the access needed to perform job functions;
- encrypt certain sensitive data;
- effectively monitor changes on its mainframe; and
- physically protect its computer resources.

A key reason for these weaknesses is that IRS has not yet fully implemented its agencywide information security program to ensure that controls are appropriately designed and operating effectively. Specifically, IRS did not annually review risk assessments for certain systems, comprehensively test for certain controls, or always validate the effectiveness of remedial actions. Until these weaknesses are corrected, the agency remains particularly vulnerable to insider threats and IRS is at increased risk of unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as inadvertent or deliberate disruption of system operations and services.

To view the full product, including the scope and methodology, click on GAO-09-136. For more information, contact Nancy Kingsbury at (202) 512-2700 or kingsburyn@gao.gov or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.