

Topics:

[Security plan](#) <sup>[2]</sup>, [deployment](#) <sup>[3]</sup>  
**[System Security Plans](#) [1]**

SS-08-028 System Security Plans

Issue Date: 3/31/2008

Revision Effective Date: 3/31/2008

## PURPOSE

System security planning is an important activity in the system development lifecycle and should be ongoing throughout the system's lifecycle so that events such as system changes or new threats trigger the need for updated security controls that can be accurately documented and effectively managed.

The purpose of the system security plan is to provide a documented overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should accurately reflect the most current state of the system.

Oversight and independent audit groups use security plan documentation to make an assessment of the management, operational and technical controls detailed in the security plan and to verify that system management has done an adequate job to highlight areas where security may be lacking and to accurately reflect how the system is actually being operated. It also provides a basis for senior management officials to make informed, risk-based decisions to authorize a system to operate.

**Supplemental Authority:** OCGA 50-18-72(a)(15)(A) Public disclosure shall not be required for records that the disclosure of which would compromise security against sabotage or criminal or terrorist acts and the nondisclosure of which is necessary for the protection of life, safety, or public property, which shall be limited to the following: (i) Security plans and vulnerability assessments for any public utility, technology infrastructure, building, facility, function, or activity in effect at the time of the request for disclosure or pertaining to a plan or assessment in effect at such time.

## STANDARD

System security requirements and controls shall be planned for, managed and documented throughout the system lifecycle.

System security plans shall reflect input from various system stakeholders, including information owners, system owner and the agency information security officer.

Security plans are living documents that shall be developed, reviewed and updated throughout the systems lifecycle to accurately reflect the current state of the information system.

Security plans contain sensitive information and shall be protected from unauthorized access and disclosure. (Reference: Supplemental Authority)

Security plans shall contain the following details in accordance with NIST SP800-18: