

Office of Management and Budget M-06-16 Mandate requires agencies to establish safeguards for sensitive agency data on laptops and workstations. To achieve compliance with the M-06-16 Mandate, agencies must enforce security measures that safeguard the integrity and availability of sensitive agency information at the endpoint.

Sanctuary Helps Agencies Comply with M-06-16 for Endpoint Security

Sanctuary ensures confidentiality and integrity of agency data on laptops and workstations by enforcing encryption when copied to removable media and by controlling what devices are used by whom and on what machines. Sanctuary helps agencies prove M-06-16 compliance through bi-directional Shadowing capabilities which detail what information has been transferred to and from a workstation to removable media. With Sanctuary, only authorized users can copy data onto encrypted removable media with complete auditing of that action.

By employing a whitelist approach, Sanctuary is uniquely capable of enforcing application and device usage and control policies, which enables only authorized applications and devices to run or connect to a network, server, terminal services server, laptop, thin client or desktop – facilitating security and systems management, while providing necessary flexibility to the agency to easily enable the use of new/upgraded applications or devices.

Through policy-based control at the endpoints to monitor and control the inbound and outbound flow of sensitive agency information, Sanctuary complements organizations' M-06-16 compliance strategy by implementing the proper internal safeguards around application and removable device use:

M-06-16 Requirement

1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive.
2. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

How Sanctuary Addresses M-06-16 Requirements

1. Sanctuary secures sensitive agency data by encrypting data that is moved onto a removable device.
2. Sanctuary provides comprehensive audit logs that detail what data has been moved onto a specific device and by which user.