HHS-OIG Cybersecurity Toolkit

Cybersecurity Considerations For HHS's Rapid Rollout of Information Systems

HHS and its Operating and Staff Divisions use information systems to help administer programs that protect the health of all Americans and provide essential human services. In response to disasters and public health emergencies, there may be a need to rapidly deploy a new information system or application to support mission-essential activities. Given the importance of the systems and sensitive data that they hold, it is critical that the systems be properly secured from bad actors who attempt to access, steal, or destroy the information.

HHS-OIG created this toolkit to help HHS leaders improve or maintain effective cybersecurity posture of systems or applications that are being rolled out. As a resource, the toolkit identifies key questions and considerations that HHS leaders should think about. These key questions and considerations are based on cybersecurity standards that HHS-OIG has used in its work assessing HHS information systems. HHS leaders should consider these cybersecurity standards when rapidly rolling out a new or modified system or application. The toolkit is not intended to comprehensively cover or ensure compliance with all Federal or HHS-specific information technology (IT) or cybersecurity requirements. Rather, HHS leaders can use it to coordinate and inform discussions within the Department and with other stakeholders about cybersecurity when rapidly planning and deploying or modifying information systems.

As HHS leaders plan their strategy to rapidly roll out an information system, below are a few questions to consider:

Who?

Who should be at the table to help plan and deploy the information system (e.g., chief information officers (CIOs), chief information security officers (CISOs), system and/or business owners, users, IT operations, attorneys, other information management and cybersecurity professionals, etc.)?

Why?

Why is the agency selecting this product? Does this decision exceed the agency's existing risk tolerance? Does the agency have a viable in-house alternative?

When?

When will the information system be deployed? When will all required cybersecurity controls testing be conducted, and will the failed controls be remediated, or untested controls be addressed to reduce risk? Has the agency planned for contingencies and implemented compensating controls for failed controls or waivers while awaiting completion of cybersecurity controls testing?

Where?

Where will sensitive information be maintained? If it's stored in a third-party system, what are the agency's baseline (or minimum) cybersecurity requirements during certain implementation phases or at key milestones (e.g., when the system goes live, or when data is downloaded)?

What?

What influence or effect does the new or modified information system have on the agency's risk tolerance and cybersecurity posture? What minimum cybersecurity requirements must the new system meet? Will the system be consistent with the agency's existing IT portfolio? Will the system contain or transmit sensitive data?

Cybersecurity Considerations For HHS's Rapid Rollout of Information Systems

Use of Existing or In-House Information Systems

HHS leaders may choose to use and rapidly modify an existing information system to capture, process, or maintain new data to meet an urgent mission need or respond to a public health emergency. As HHS leaders plan for, modify, and deploy new functionalities in their existing information system, the following four courses of action should be considered to ensure an effective cybersecurity posture.

Develop a timeline for information system deployment, including developing timeframes for conducting minimum cybersecurity testing. Consult with cybersecurity subject matter experts, such as your CIO or CISO, DHS CISA, and NIST to ensure that testing is documented and based on sound cybersecurity standards (e.g., NIST SP 800-53).

Assess whether the modification impacts the existing information system's "cybersecurity baseline categorization" and risk exposure using cybersecurity standards (e.g., NIST SP 800-53 and FIPS 199).

Identify existing controls and determine if the controls are appropriate and operating effectively to identify and prevent or minimize cybersecurity issues. This should include testing access controls and account management processes (e.g., determining if access controls or user access rights need to be modified and ensuring compliance with account management principles of "need to know" and "least privilege").

Determine whether existing contingency plans and back-up procedures will be impacted by the modifications and therefore require updating. Ensure that continuity of operations plans are in place to allow mission-essential functions to continue should a disruption occur.

Cybersecurity Considerations For HHS's Rapid Rollout of Information Systems

Use of a Commercial Off-The-Shelf Product

HHS leaders may acquire commercial off-the-shelf products to rapidly roll out a new information system or cloud service. The new system or service may be used to support the collection or processing of new information, replace current systems, or connect with other information systems. As HHS leaders plan for and roll out new information systems or cloud services using commercial off-the-shelf products, they should conduct the following activities to ensure an effective cybersecurity posture.

When considering a commercial off-the-shelf product from a contractor or vendor, specify in the contract that the contractor must meet the applicable Federal IT security requirements and regulations (e.g., OMB, FISMA, or NIST SP) prior to processing Federal information, and that the commercial off-the-shelf product must meet required industry standards, as applicable.

Develop a timeline for cybersecurity testing (e.g., user and controls testing), including documenting the test plans and results. For the testing, consider:

- Are there third-party tests that can be relied on to minimize cybersecurity testing (e.g., testing by third-party testing/assessment organizations)?
- What type of cybersecurity controls testing will be performed (e.g., vulnerability scans or penetration testing)? If you rely on third-party testing, what type of verification will be performed to obtain assurance that the testing was adequate and information system is secure? If testing was not adequate or the system is not secure, what should be done? Is the CISO or CIO (or equivalent official) in agreement?

Assess insider risk (e.g., determine who will access the information system and ensure compliance with the account management principles of "need to know" and "least privilege").

Determine how the new information system will be included in existing contingency plans and back-up procedures.

- What contingency plans or procedures need updating with the change?
- Where are back-ups stored? Can the information system be recovered at a geographically separate alternate site?

After cybersecurity testing is completed and management has signed off on the risks, maintain cybersecurity in accordance with the Federal and industry cybersecurity requirements. Conduct full and periodic cybersecurity assessments, including periodically assessing access controls and account management.