RAPID7

NIST 800-171 EXPLAINED

How the Rapid7 Portfolio Can Help You Achieve Compliance with NIST Special Publication 800-171

Last updated: October 2017

TABLE OF CONTENTS

WHAT ARE THE NIST FRAMEWORKS FOR DATA SECURITY?

The National Institute of Standards and Technology (NIST) developed three documents around data security controls.

NIST 800-53 and **NIST 800-171** are both catalogs of data security controls. U.S. federal agencies use 800-53, and various versions of it have been in effect for years. 800-171 applies to organizations that either work with the U.S. government or handle sensitive government data, and those organizations have a deadline to implement NIST 800-171 by the end of 2017 (the "DFARS" regulation, which we will address shortly). The **Cybersecurity Framework** (CSF), in contrast, is a shorter, generalized document that outlines approaches to cybersecurity risk any organization could undertake.

All three aim to build a more structured approach to cybersecurity risk, and the many internal controls an organization can implement to manage it. They all work toward the same capabilities: identify risks and assets; protect assets; detect threats; respond to threats; and, should the worst happen, recover from attacks.

The NIST frameworks for data security are grouped into three documents:

NIST 800-53

What it is: Helps federal agencies implement proper controls as required under FISMA.

Who it applies to: Federal agencies.

NIST 800-171

What it is: A subset of NIST 800-53; used to demonstrate compliance with DFARS for handling Controlled Unclassified Information (CUI).

Who it applies to: Organizations that work in the US government or handle sensitive government data.

Cybersecurity Framework (CSF)

What it is: Document outlining organizational approach to cybersecurity risk.

Who it applies to: It's voluntary, but is useful for any organization, particularly critical infrastructure sectors such as banking or public utilities.

WHO NEEDS TO BE NIST COMPLIANT AND WHY?

All federal agencies are expected to use NIST 800-53, formally titled "Security and Privacy Controls for Federal Information Systems and Organizations," to understand what data security controls they should put in place, depending on the information systems they use and the sensitivity of data on their networks. 800-53 has gone through several incarnations. The current version, Revision 4, has been in effect since 2013; a fifth revision is out for public comment now. (We will discuss Revision 5 shortly.)

NIST 800-171 is essentially a subset of 800-53, intended for government contractors and other organizations (research universities or nonprofits, for example) that might handle Controlled Unclassified Information (CUI) as part of their operations. In December 2015, the Department of Defense (DoD) published an addendum to DFARS (252.204.7012) specifying 800-171 as the cybersecurity framework government contractors must implement if they handle CUI. This set a deadline for all parties handling CUI to implement the controls of 800-171 prior to Dec. 31, 2017. After that, non-compliant organizations will be at risk of losing their contracts.

REQUIREMENTS FOR U.S. GOVERNMENT ORGANIZATIONS (NIST 800-53)

NIST 800-53 runs 462 pages in total. It isn't a framework in the strict sense, but rather a catalog of eighteen "control families," with a varying number of specific controls in each family. These will feel familiar to most security, compliance, and audit professionals.

The control families include:

- Access control
- Awareness and training
- Configuration management
- Incident response
- Security assessment

Take access controls, the "AC" family, as an example. It has 25 controls. AC-1 is an entity-level control: policies and procedures. The organization will create, document, and disseminate an access control policy, as well as procedures to put that policy (and any associated controls) into force. Meanwhile, AC-7 is an operational control: limit the number of unsuccessful log-in attempts. An additional AC-7(2) requires wiping sensitive data from a mobile device after a set number of unsuccessful attempts.

The PL control family, in contrast, addresses planning: that an organization adopts policies and procedures for security, defines roles and responsibilities, disseminates those policies and procedures to the proper people, and so forth. PL-4 requires "rules that describe their responsibilities and expected behavior" (essentially, a Code of Conduct); and a sub-control defines the certifications users should submit to indicate that they understand those rules.

Revision 4 is the current version of 800-53. NIST had published a draft of Revision 5, out for public comment through Sept. 12, 2017. The draft is 494 pages. One of its primary goals is to address the "Internet of Things" (IoT) world that has emerged. That IoT environment has made personally identifiable information (PII) more vulnerable because that data can be stored on more devices. One proposed change in Revision 5 is the tighter integration of privacy and security controls, to be more reflective of modern IoT security architecture.

Revision 5 would also aim for easier integration with CSF or other risk management frameworks that organizations might use, whether they are government agencies or not. Indeed, one telling proposal is to drop the word "federal" from the title, to convey the idea that 800-53 Revision 5 can apply to any organization.

REQUIREMENTS FOR ORGANIZATIONS HANDLING CUI (NIST 800-171)

NIST 800-171 is shorter and simpler than 800-53: It contains 110 controls across 14 control families, in a publication only 76 pages long. Many businesses will need to demonstrate compliance with NIST 800-171 to participate in government contracts or to do business with other companies in critical infrastructure sectors.

As cybersecurity becomes an enormous part of third-party risk, this means that strong, documented, tested cybersecurity controls won't only protect your organization—they will make you a more attractive third party to other business partners.

Given the relatively new requirement for many organizations to prove compliance from 2018 onward, the controls of NIST 800-171 have become a very important measure for security programs. These controls may span processes and technologies, but it can be difficult to identify which security vendor can help your organization with each. Once you have mapped what you have in place to identify your remaining controls gaps, it is important to define your plan for filling them in a reasonable timeframe. Our hope is that this document provides the transparency your organization seeks from a security vendor.

HOW RAPID7 CAN HELP

Rapid7 has extensive experience partnering with public and private sector organizations, such as Raytheon, Northrop Grumman, and Lockheed Martin. Rapid7 has software solutions spanning a large portion of the NIST frameworks, as well as the consulting services to help organizations measure against and develop a plan to complete their implementation.

Rapid7 InsightVM and Nexpose are vulnerability management solutions that help organizations find and fix vulnerabilities, misconfigurations, and exposures from the endpoint to the cloud.

In the context of NIST 800-171, our vulnerability management solutions help covered entities to:

- Perform quarterly internal and external vulnerability scanning of their environment.
- Implement secure configuration policies based on industry standards like CIS and DISA STIG.
- Identify and prioritize vulnerabilities based on threat exposure and asset criticality.
- Audit system access, authentication and other security controls to detect policy violations.
- Automatically detect and scan new devices as they enter the network.
- Create, assign, track and verify remediation tasks.
- Demonstrate compliance and communicate progress with reports, analytics, and live dashboards.

Rapid7 Metasploit is a penetration testing solution that provides risk assessment through the controlled simulation of a real-world attack.

In the context of NIST 800-171, Metasploit helps covered entities to:

- Perform internal and external penetration tests on their network.
- Validate effectiveness of network segmentation controls.
- Test access and authentication control systems and policies.
- Simulate password attacks to identify weak and shared credentials.
- Prioritize critical risks with closed-loop vulnerability validation.
- Simulate phishing campaigns to measure security awareness.

Rapid7 InsightAppSec and AppSpider are dynamic application security testing (DAST) solutions that assess web, mobile, and cloud applictions for vulnerabilities across all modern technologies.

In the context of NIST 800-171, our application security solutions covered entities to:

- Automatically simulate attacks to test web applications.
- Identify gaps in compliance with best practices for secure software development.
- Integrate application security testing throughout the software development lifecycle.
- Continuously monitor applications for changes.
- Automatically generate targeted WAF/IPS rules.
- Identify web application vulnerabilities that allow unauthorized or insecure access.

Rapid7 InsightIDR is a complete incident detection and response solution that goes beyond traditional SIEM capabilities to combine compliance dashboards, log aggregation, user behavior analytics, endpoint interrogation, and real-time search.

In the context of NIST 800-171, InsightIDR helps covered entities to:

- Audit the separation between development/test and production environments.
- Monitor access to cardholder data to ensure the user's job requires access.
- Expose risky user behavior, including shared user accounts, non-expiring passwords, and anomalous administrative activity.
- Aggregate and correlate log files from an existing network and security stack (e.g. IDS/IPS, Firewall, Event logs) directly to the users and assets behind them.
- Enable the security team to combine log search, real-time user activity, and endpoint artifacts together on a Super Timeline during incident investigations.
- Track user authentications and admin activity across local, domain, and cloud services.
- Monitor disabled users and service accounts across on-premise and cloud systems to identify compromised credentials and lateral movement.
- Audit access to restricted assets.
- Alert the security team on top attack vectors behind breaches, including stolen credentials, phishing, and malware.

Rapid7 InsightOps is an IT Operations solution that automatically combines live log management and asset data from across an organization's infrastructure into one central and searchable location, so they can easily access the insight they need, when they need it.

In the context of NIST 800-171, InsightOps helps covered entities to:

- Confirm that there are no shared accounts and that normal and elevated administrative privileges are linked to individual, trackable users.

- Ensure audit trails exist for all individual accesses to cardholder data, administrative and root access actions, creation and deletion of system-level objects, and invalid logical access attempts.
- Record audit trail entries for all system components for each event, including event type, date and time, origination of event, and more.

Rapid7 offers a variety of **Managed and Consulting Services** to help organizations accelerate security improvement through industry-leading methodologies and experts who understand the attacker mindset. In addition to Consulting services, Rapid7 also offers managed versions of its software products listed above.

In the context of NIST 800-171, the Rapid7 Managed and Consulting Services teams help covered entities to:

- Develop and manage a vulnerability management program.
- Perform penetration testing on networks, applications, and users (social engineering).
- Build a penetration testing methodology.
- Perform a security program assessment to determine if security policies and procedures are being followed in actual day-to-day operations, identify gaps in their security program, and provide guidance on developing missing control policies and procedures.
- Provide customizable security awareness training to users.
- Build an incident response plan and simulate breach scenarios to increase readiness.
- Detect and analyze threats in real-time, then investigate and remediate incidents.

RAPID7 SOLUTIONS FOR NIST 800-171 COMPLIANCE

This section details the NIST 800-171 security requirements and how Rapid7 products and services help organizations become and remain compliant.

NIST 800-171		InsightVM* or Nexpose	Metasploit	InsightOps	InsightIDR	InsightAppSec or AppSpider	Managed or Consulting
Requirement 3.1	Access Control	x	-	-	x	-	-
Requirement 3.2	Awareness and Training	-	x	-	-	-	-
Requirement 3.3	Audit and Accountability	-	-	x	x	-	-
Requirement 3.4	Configuration Management	x	-	x	x	-	-
Requirement 3.5	Identification and Authentication	x	-	-	x	-	-
Requirement 3.6	Incident Response	-	x	-	-	-	x
Requirement 3.7	Maintenance	-	-	-	-	-	x
Requirement 3.8	Media Protection	-	-	-	x	-	-
Requirement 3.9	Personnel Security	-	-	-	-	-	-
Requirement 3.10	Physical Protection	-	-	-	-	-	-
Requirement 3.11	Risk Assessment	x	-	-	-	x	x
Requirement 3.12	Security Assessment	x	x	-	x	-	x
Requirement 3.13	System and Communications Protection	-	-	-	x	x	-
Requirement 3.14	System and Information Integrity	-	-	-	x	x	-

**Our award-winning Nexpose product has evolved into InsightVM, which utilizes the power of the Rapid7 Insight platform, our cloud-based security and data analytics solution.*

Requirement 3.1 - Access Control

3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
3.1.3	Control the flow of CUI in accordance with approved authorizations.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
3.1.8	Limit unsuccessful logon attempts.
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.
3.1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.
3.1.11	Terminate (automatically) a user session after a defined condition.
3.1.12	Monitor and control remote access sessions.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
3.1.14	Route remote access via managed access control points.
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.
3.1.16	Authorize wireless access prior to allowing such connections.
3.1.17	Protect wireless access using authentication and encryption.
3.1.18	Control connection of mobile devices.
3.1.19	Encrypt CUI on mobile devices.
3.1.20	Verify and control/limit connections to and use of external information systems.
3.1.21	Limit use of organizational portable storage devices on external information systems.
3.1.22	Control information posted or processed on publicly accessible information systems.

Use Rapid7 InsightVM or Nexpose to:

- Enable users to see only the vulnerabilities for systems they need access to using robust role-based access control. (Requirement 3.1.1)
- Limit what actions users can take with which assets in InsightVM and Nexpose, such as limiting users to only be able to scan their own assets. (Requirement 3.1.2 and 3.1.4)
- Organize remediation by role and responsibility, so you can see which team members are responsible for which systems. (Requirement 3.1.3)
- Limit what actions users can take with which assets in InsightVM and Nexpose, such as limiting only specific people to be able to run scans and generate reports. (Requirement 3.1.5)
- Assign accurate roles and responsibilities to everyone involved in the vulnerability management program using flexible role-based access control. (Requirement 3.1.6)

Use Rapid7 InsightIDR to:

- Detect non-privileged users performing administrative actions, whether they are a compromised user or a malicious insider. (Requirement 3.1.7)
- Detect multiple forms of password guessing attempts, whether it be a standard bruteforce, a striping attack (horizontal bruteforce), pass-the-hash, or even if the authentication was successful but likely from a stolen credential. (Requirement 3.1.8)
- Give security teams visibility into remote access sessions from VPN, cloud services, or from traveling/remote endpoints with included endpoint monitoring. (Requirement 3.1.12)
- Run forensic jobs for incident investigation using the Insight Agent, such as to pull registry data, prefetch information, or identify scheduled tasks. (Requirement 3.1.15)
- Monitor authentications coming onto the network from mobile devices, such as when they enter via VPN, cloud services, or Outlook Web Access (OWA). (Requirement 3.1.18)
- Identify and alert on use of portable storage devices on endpoints via the included Insight Agent. (Requirement 3.1.21)

Requirement 3.2 - Awareness and Training

3.2.1	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.
3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Use Rapid7 Metasploit Pro to:

- Send and track emails to thousands of users with phishing campaigns, and direct security awareness training by measuring conversion rates at each step in the social engineering campaign funnel. (Requirement 3.2.1)

Requirement 3.3 - Audit and Accountability

3.3.1	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
3.3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
3.3.3	Review and update audited events.
3.3.4	Alert in the event of an audit process failure.
3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.
3.3.7	Provide an information system capability that compares and synchronizes internal systsem clocks with an authoritative source to generate time stamps for audit records.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.
3.3.9	Limit management of audit functionality to a subset of privileged users.

Use Rapid7 InsightIDR to:

- Provide complete centralized log management, including log search, data visualization, and compliance reporting. Any log source can be sent to be made available for search and securely stored on the Insight platform. (Requirement 3.3.1)

- Automatically detect attacks by applying user behavior analytics to InsightIDR data. This context is presented in a visual timeline to accelerate investigations. (Requirement 3.3.1)

- Ingest data across network, endpoint, and cloud data sources. All of these actions are attributed to the users behind them. No more retracing IP addresses to assets and users or consulting multiple tools for slivers of context. (Requirement 3.3.2)

- Effectively parse large amounts of data using the Log Entry Query Language (LEQL), and to surface and dig through anomalies without writing any LEQL at all by using Visual Search. (Requirement 3.3.3)

- Create custom alerts—this can alert in the event of an audit process failure, or the failure of a data source to send information to the Insight platform. (Requirement 3.3.4)

- Surface misconfigurations and malicious activity through a range of pre-built detections. From there, you can investigate the incident through a visual timeline. Additional sources of data, such as from logs and endpoints, can be added to the investigation. (Requirement 3.3.5)

- Leverage the pre-built compliance cards and a flexible card creation system. (Requirement 3.3.6)
- Securely send your audit information to the Insight platform, where the architecture keeps your data private, secure, and highly available. (Requirement 3.3.8)
- Allow users to view information without disrupting workflows or data based on multiple levels of role-based access. (Requirement 3.3.8 and 3.3.9)
- Accelerate the audit process with the robust log search and pre-built compliance cards. (Requirement 3.3.9)
- Ensure only authorized users are accessing InsightIDR by supporting multi-factor authentication. (Requirement 3.3.9)

Use Rapid7 InsightOps to:

- Provide complete centralized log management, including log search, data visualization, and compliance reporting. Any log source can be sent to be made available for search and securely stored on the Insight platform. (Requirement 3.3.1)
- Effectively parse large amounts of data using the Log Entry Query Language (LEQL), and to surface and dig through anomalies without writing any LEQL at all by using Visual Search. (Requirement 3.3.3)

Requirement 3.4 - Configuration Management

3.4.1	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational information systems.
3.4.3	Track, review, approve/disapprove, and audit changes to information systems.
3.4.4	Analyze the security impact of changes prior to implementation.
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
3.4.6	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.
3.4.7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.
3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or denyall, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
3.4.9	Control and monitor user-installed software.

Use Rapid InsightVM or Nexpose to:

- Scan systems for adherence to configuration policies like DISA STIG and CIS. (Requirement 3.4.1 and 3.4.2)
- Create an inventory of all systems scanned. (Requirement 3.4.1)
- Scan systems to ensure only certain ports and services are being used, and to help you adhere to policies like CIS for limiting these functions. (Requirement 3.4.6)

Use Rapid7 InsightIDR to:

- Identify misconfigurations and risk in your environment. For example, you'll be able to see accounts with passwords set to never expire, admin privileges across your users, and the cloud services and processes being accessed from your endpoints. (Requirement 3.4.2)
- Logically label different systems or business groups based on IP ranges. Define these network zones, such as Production and Development, and be alerted on exceptions to enforce your security policies. (Requirement 3.4.5)
- Identify administrators and admin actions taken across the network, endpoint, and cloud services. This helps enforce least-privilege by exposing unknown admins and alerting you when anomalous admin actions take place on critical assets. (Requirement 3.4.6)
- Proactively identify all running processes on endpoints across your organization. Unique and rare processes are surfaced, allowing you to identify Shadow IT and malware never before seen in the wild. (Requirement 3.4.9)

Use Rapid7 InsightOps to:

- Report if unauthorized software is installed on an asset. (Requirements 3.4.8)
- Query assets in the environment and report on installed software on an asset-by-asset basis or in aggregate. (Requirement 3.4.9)

Requirement 3.5 - Identification and Authentication

3.5.1	Identify information system users, processes acting on behalf of users, or devices.
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
3.5.3	Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
3.5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.
3.5.5	Prevent reuse of identifiers for a defined period.
3.5.6	Disable identifiers after a defined period of inactivity.
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.
3.5.8	Prohibit password reuse for a specified number of generations.
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.
3.5.10	Store and transmit only encrypted representation of passwords.
3.5.11	Obscure feedback of authentication information.

Use Rapid7 InsightIDR to:

- Integrate with your existing network and security stack to monitor your complete environment. This includes user activity, processes, and activity on endpoints and cloud services. This behavior is baselined and helps identify anomalous and malicious stealthy attacker activity. (Requirement 3.5.1)
- Tag important assets in your environment as critical. Any authentications to those assets from anomalous users or source assets triggers an automatic alert. (Requirement 3.5.2)

Use Rapid7 InsightVM or Nexpose to:

- Scan systems for password policy compliance to make sure they meet complexity and age policies. (Requirement 3.5.7 and 3.5.8)

Requirement 3.6 - Incident Response

3.6.1	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.
3.6.3	Test the organizational incident response capability.

Use Rapid7 Managed or Consulting Services to:

- Receive 24/7 coverage from an experienced Managed Detection and Response (MDR) team that has responded to thousands of breaches. In addition to monitoring, our analysts perform a compromise assessment to ensure no existing or prior breach, and proactively hunt across the network. With Rapid7 MDR, incident escalation is included in the service. Rapid7 can easily pivot from detection to response and has a deep understanding of customer environments. This saves time and money as the Rapid7 MDR team is immersed in the nuances that a third-party team would need additional time to learn and adapt to, including acquisitions. (Requirement 3.6.1)
- Receive on-site threat simulation to evaluate detection and response capabilities in a controlled environment via tabletop exercises. The Rapid7 team works with customers to create and deliver a meaningful scenario, analyze the results, and provide a list of actionable improvements that apply to your incident response program. (Requirement 3.6.1 and 3.6.3)
- Build or improve capabilities in any area of the Security Program Lifecycle (Preparation, Prevention, Detection, Response, Remediation, Cleanup, Lessons Learned) through customizable Rapid7 Incident Response Program Development services. Rapid7 experts evaluate the customer environment—from technology to assets to people, process, and policy—to rate capability and offer relevant, business-based recommendations to help organizations meet their IR program goals. This service can assist customers looking to build their IR program from the ground up. (Requirement

3.6.1)

- Build or improve capabilities in any area of the Security Program Lifecycle—including the Response, Remediation, and Cleanup phases used for tracking, documenting, and reporting security incidents—through customizable Rapid7 Incident Response Program Development services. (Requirement 3.6.2)
- Work hand-in-hand with Rapid7 Incident Response consultants and your own team during a Red/Blue Team Exercise to assess and provide guidance around detection and response tools and procedures, all while Rapid7 penetration testers simulate attacks. (Requirement 3.6.3)

Use Rapid7 Metasploit Pro to:

- Test the effectiveness of their security controls and processes while increasing penetration testers' productivity, validating vulnerabilities, and improving security awareness. (Requirement 3.6.3)

Requirement 3.7 - Maintenance

3.7.1	Perform maintenance on organizational information systems.
3.7.2	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in the information system.
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.

Use Rapid7 Consulting Services to:

- Receive a Cyber Security Maturity Assessment (CSMA), a gap analysis and risk assessment that utilizes cybersecurity best practices and recognized cyber frameworks. The goal of the CSMA is to provide organizations with a view of their current security posture, an objective review of existing plans, and a guide to strategic planning. The CSMA also helps organizations develop tactical and strategic plans to further mature and strengthen security program efforts. (Requirement 3.7.1)

Requirement 3.8 - Media Protection

3.8.1	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.
3.8.2	Limit access to CUI on information system media to authorized users.
3.8.3	Sanitize or destroy information system media containing CUI before disposal or release for reuse.
3.8.4	Mark media with necessary CUI markings and distribution limitations.

3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
3.8.7	Control the use of removable media on information system components.
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.
3.8.9	Protect the confidentiality of backup CUI at storage locations.

Use Rapid7 InsightIDR to:

- Identify the use of removable media on information systems. Through the Insight Agent, which provides endpoint detection and visibility, you can be alerted each time a USB key is inserted into the critical asset. (Requirement 3.8.7)

Requirement 3.11 - Risk Assessment

3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.
3.11.2	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.
3.11.3	Remediate vulnerabilities in accordance with assessments of risk.

Use Rapid7 Consulting Services to:

- Receive a Cyber Security Maturity Assessment (CSMA), a gap analysis and risk assessment that utilizes cybersecurity best practices and recognized cyber frameworks. The goal of the CSMA is to provide organizations with a view of their current security posture, an objective review of existing plans, and a guide to strategic planning. The CSMA also helps organizations develop tactical and strategic plans to further mature and strengthen security program efforts. (Requirement 3.11.1)

Use Rapid7 InsightVM or Nexpose to:

- Scan a wide variety of systems for vulnerabilities, and can also be set up to automatically scan systems for new critical vulnerabilities as they're released. (Requirement 3.11.2)

- Receive remediation reporting based on which steps reduce the most overall risk in your environment. InsightVM's remediation workflows take this approach with additional live monitoring and integration with ticketing systems like JIRA and ServiceNow. (Requirement 3.11.3)

Use Rapid7 InsightAppSec or AppSpider to:

- Dynamically test web applications for security vulnerabilities and set it up to scan applications on a recurring schedule or to be triggered automatically by processes in the software development lifecycle. (Requirement 3.11.2)

- Receive detailed technical information for each identified vulnerability, as well as remediation recommendations so that development and devops teams have the information needed to make the code or configuration changes needed to remediate a vulnerability. (Requirement 3.11.3)

Requirement 3.12 - Security Assessment

3.12.1	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
3.12.3	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Use Rapid7 Consulting Services to:

- Receive a Cyber Security Maturity Assessment (CSMA), a gap analysis and risk assessment that utilizes cybersecurity best practices and recognized cyber frameworks. The goal of the CSMA is to provide organizations with a view of their current security posture, an objective review of existing plans, and a guide to strategic planning. The CSMA also helps organizations develop tactical and strategic plans to further mature and strengthen security program efforts. (Requirement 3.12.1)

- Evaluate and test the comprehensiveness and effectivness of security controls by leveraging Rapid7 Tabletop Exercises, Penetration Testing Services, and Cyber Security Maturity Assessments. (Requirement 3.12.3)

Use Rapid7 Metasploit Pro to:

- Enable teams to test the effectiveness of their security controls and processes while increasing penetration testers' productivity, validating vulnerabilities, and improving security awareness. (Requirement 3.12.1 and 3.12.3)

Use Rapid7 InsightVM to:

- Create detailed remediation projects to plan and monitor remediation efforts. Live dashboards provide trending analysis to help plan strategic initiatives for reducing risk. (Requirement 3.12.2)

Requirement 3.13 - System and Communications Protection

3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.
3.13.3	Separate user functionality from information system management functionality.
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.

3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
3.13.10	Establish and manage cryptographic keys for cryptography employed in the information system.
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
3.13.13	Control and monitor the use of mobile code.
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
3.13.15	Protect the authenticity of communications sessions.
3.13.16	Protect the confidentiality of CUI at rest.

Use Rapid7 AppSpider to:

- Integrate with several Web Application Firewalls, generating technical rules based on AppSpider-identified vulnerabilities that the WAF can use to protect against attacks that target said vulnerabilities. (Requirement 3.13.1)

Use Rapid7 InsightIDR to:

- Identify unauthorized information transfer via shared system resources. In file shares, you can tag items as "Honey Files"—you'll receive an automatic alert if items in that directory are opened, copied, or edited. (Requirement 3.13.4)

Requirement 3.14 - System and Information Integrity

3.14.1	Identify, report, and correct information and information system flaws in a timely manner.
3.14.2	Provide protection from malicious code at appropriate locations within organizational information systems.
3.14.3	Monitor information system security alerts and advisories and take appropriate actions in response.
3.14.4	Update malicious code protection mechanisms when new releases are available.
3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
3.14.6	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
3.14.7	Identify unauthorized use of the information system.

Use Rapid7 InsightAppSec or AppSpider to:

- Dynamically test web applications for security vulnerabilities, including those that put CUI at risk. Detailed technical information on identified vulnerabilites and recommendations are provided to remediate the vulnerability. Reports of vulnerabilities including those that relate to specific compliance requirements can also be generated. (Requirement 3.14.1)

Use Rapid7 AppSpider to:

- Integrate with several Web Application Firewalls, generating technical rules based on AppSpider-identified vulnerabilities that the WAF can use to protect against attacks that target said vulnerabilities. (Requirement 3.14.2)

Use Rapid7 InsightIDR to:

- Ingest alerts from other security tools, such as anti-virus, firewall, and web proxy. Additional user context is layered onto the alert, helping you make informed investigation decisions faster. (Requirement 3.14.3)
- Detect unauthorized use of information systems in real-time. This includes both malware and commoditized attacks, as well as the use of stolen credentials to gain unauthorized access. (Requirement 3.14.7)

ABOUT RAPID7

With Rapid7 (NASDAQ: RPD), security and IT professionals gain the clarity and confidence they need to protect against risk and drive innovation Rapid7 analytics transform data into answers, eliminating blind spots and giving customers the insight they need to securely develop and operate today's sophisticated IT infrastructures, networks, and applications, Rapid7 solutions include vulnerability management, penetration testing, application security, incident detection and response, SIEM and log management, and offers managed and consulting services across its portfolio. To learn more about Rapid7 or get involved in our threat research, www.rapid7.com.