At Rapid7, supporting our customers and prospects encompasses more than just providing products and services; it is a partnership built on trust. As our CEO Corey Thomas noted, the industry must move away from treating security as an "add-on" or a profit center. For all of us at Rapid7, Security is part of our DNA—not just in the solutions we sell, but in how we build and operate them under the highest levels of scrutiny.

We are proud to proactively participate in the CISA Secure by Design Pledge as tangible evidence of our dedication to establishing industry-leading best practices. This commitment ensures that we are not just reacting to threats, but engineering them out of the ecosystem entirely.

Below are the details on our progress toward achieving the CISA 7 Goals, demonstrating our continued drive to maintain high-quality, resilient products that prioritize the safety of our customers' data above all else.

1. Multi-factor Authentication(MFA)

Goal: Demonstrate actions taken to measurably increase the use of multifactor authentication across the manufactufacturer's products.

How we are meeting this goal: The Rapid7 Command Platform provides Multi-factor authentication (MFA) as a mandatory security layer to ensure secure access to platform products and data. Once MFA is enabled, customers can choose from various available options—including industry-approved app-generated passcodes and push notifications—and configure additional settings for users.

Internally, our S-SDLC Standard enforces MFA across all segmented cloud environments, including development, test, and production. We further protect the software supply chain by requiring that all development signing private keys be stored in secure, MFA-protected vaults.

In direct alignment with **OMB M-22-09**, Rapid7 is prioritizing the transition toward phishing-resistant authentication methods, such as FIDO2 and WebAuthn. Additionally, we support government-mandated PIV and CAC card integration through single sign-on partnerships with industry-approved providers. This ensures that both internal and external managed applications meet the highest federal identity standards.

2.Default Passwords

Goal: Within one year of signing the pledge, demonstrate progress towards reducing default passwords across the manufacturer's products.

How we are meeting this goal: Rapid7 enforces a robust password policy architecture that aligns with industry best practices and the Federal **Zero Trust Architecture**. The Rapid7 Command Platform eliminates the risk of universally shared credentials by utilizing unique, invitation-based provisioning for every user. This ensures that only the customer possesses their authentication credentials from the moment of account setup.

Administrators are granted the granularity to implement custom configurations that exceed standard benchmarks. These include the ability to mandate a minimum password length of 12 or 16 characters, and enforce password history for up to 12 iterations to prevent reuse. Our platform further enhances security by prohibiting the use of any part of the user's account email address within their password.

Under our S-SDLC Standard, we utilize Just-in-Time (JIT) access and configuration-as-code to ensure no standing credentials persist in our production infrastructure. We also require all system and vendor-supplied default accounts to have their passwords changed and subsequently disabled prior to initial deployment. These efforts are part of our broader strategic move toward a passwordless future. More information on the Rapid7 Command Platform default password policy can be found here.

3.Reducing entire classes of vulnerability

Goal: Within one year of signing the pledge, demonstrate actions taken towards enabling a significant measurable reduction in the prevalence of one or more vulnerability classes across the manufacturer's products.

How we are meeting this goal: Rapid7 engineering teams perform static code analysis (SAST) and dependency scanning across all applications to proactively identify and prevent common vulnerability classes, including SQL injections and cross-site scripting. These scans are integrated into our CI/CD pipelines as embedded security controls to ensure issues are detected before code reaches production.

Our commitment to reducing vulnerabilities is independently validated through rigorous third-party audits. Rapid7 maintains **ISO 27001** certification for its Information Security Management System (ISMS) and undergoes annual **SOC 2 Type II** audits to ensure control effectiveness.
Internally, our S-SDLC Standard explicitly prioritizes memory-safe programming languages while mandating additional testing for non-memory-safe languages. We also require formal threat modeling and secure design reviews for all new projects. To meet the transparency requirements of **Executive Order 14028**, Rapid7 provides Software Bill of Materials (SBOMs) for deep risk assessments.

4.Security Patches

Goal: Within one year of signing the pledge, demonstrate actions taken to measurely increase the installation of security patches by customers.

How we are meeting this goal: Our Information Security team monitors patching compliance using our own tools, while our platform delivery team deploys security patches on a regular basis for the Rapid7 Command Platform infrastructure. Our solutions follow a continuous deployment model that delivers software updates and security patches to all customers automatically.

The platform includes a Managed Agent Update setting that allows for the immediate, automated deployment of critical patches and independent components. This automation is specifically designed to assist federal agencies in complying with **CISA BOD 22-01**. This ensures that Known Exploited Vulnerabilities (KEVs) are remediated within the mandated timelines to minimize organizational risk. For more information, visit here.

5. Vulnerability disclosure policy

Goal: Within one year of signing the pledge, publish a vulnerability disclosure policy.

How we are meeting this goal: Rapid7 understands the importance of a clear process to report key vulnerabilities in a timely manner and maintains a formal Vulnerability Handling and Disclosure Program. We advocate for the transparent disclosure of vulnerabilities in our own platforms and in third-party products discovered within a customer's tech stack.

Our S-SDLC formally defines a Product Security Incident Response Team (PSIRT) as part of our standardized "RapidFire" incident response process. This team manages stakeholder coordination, technical analysis, and public communication. This proactive defense posture ensures that government SOCs and the broader security community are notified of risks in alignment with internal remediation requirements. Customers and any other external parties can report any known vulnerabilities to Rapid7 via our Vulnerability Handling and Disclosure Program found here.

6. CVE's

Goal: Within One year of signing the pledge, demonstrate transparency in vulnerability reporting.

How we are meeting this goal: As a leader in the security industry, Rapid7 utilizes a dedicated platform to ensure the reporting of vulnerabilities in our products and services. A cornerstone of our transparency is our status as a CVE Numbering Authority (CNA) since 2016. This allows us to assign CVE IDs directly to vulnerabilities discovered in our own products as well as those found in other vendors' products by our researchers.

We follow secure SDLC processes that prioritize all reported vulnerabilities and aim to provide research outcomes within approximately 60 days of verification. In every CVE record we publish, we commit to including accurate CWE and CPE metadata to help customers prioritize their risks effectively.

We maintain open communication regarding the progress of vulnerability disclosures and proposed fixes. Additionally, we utilize internal governance tools to track a "definition of done" for all security checks, providing the evidence and visibility required for government agencies to maintain their Authorizations to Operate (ATO). For more information visit here.

7. Evidence of intrusions

Goal: Within one year of signing the pledge, demonstrate a measurable increase in the ability for Customers to gather evidence of Cybersecurity intrusions affecting the manufacturer's products.

How we are meeting this goal: The Rapid7 Command Platform provides granular audit logging capabilities that record both user-driven and automated activity. For every auditable action, customers can see the specific action, the time it occurred, and the identity of the user involved.

In addition to customer-facing logs, our internal S-SDLC mandates the use of integrated cloud logging and threat detection services to audit privileged access and protect log data. These capabilities are designed to help customers meet their compliance obligations, including **OMB M-21-31** requirements.

This infrastructure facilitates the export of high-fidelity telemetry to government-operated SIEMs. This supports enterprise-wide threat hunting and forensic investigations to ensure the overall operational health of our customers' systems. For more information on the audit logging capabilities available in our products, visit here.