SecurID Receives FedRAMP Moderate Authorization

Federal Solution Adds 325 Controls to Secure Government's Cloud Journeys

Washington D.C. – May 4, 2022 – SecurID, the trusted identity platform and an RSA business, today announced that the Federal Risk and Authorization Management Program (FedRAMP) had approved the SecurID Federal cybersecurity solution for government use. A government-wide program, FedRAMP certifies that solutions have the core capabilities that government agencies need to secure and accelerate the adoption of cloud services. Offered via RSA Federal, SecurID's cloud-based identity and access management solution has added 325 security and privacy controls based off the NIST 800-53 framework to support U.S. government agencies and Federal System Integrators' journey to the cloud. Receiving approval following the FedRAMP certification process ensures that RSA Federal meets rigorous government security standards.

"The public sector trusts our multi-factor authentication (MFA) and identity management solutions to empower employees, partners and contractors to do more—without compromising security or convenience," said **Jim Taylor, Chief Product Officer, SecurID**. "As the trusted identity platform, we have the flexibility and focus to adapt to the needs of government agencies wherever they work—whether that's on-premises, in the cloud or both. The result of this certification has improved upon our cybersecurity software for not only government organizations, but our commercial products as well."

The pandemic, geopolitical crises, an uptick in nation-state attacks and the adoption of new technologies like cloud and 5G have driven major shifts in the threat landscape and resulted in heightened risks. Mounting threats combined with government mandates and executive orders, including Shields Up, the Strengthening American Cybersecurity Act, the Cyber Incident Reporting for Critical Infrastructure Act and many others put more pressure on government agencies and businesses alike to improve their cybersecurity posture. With SecurID's decades of history solving government security challenges, RSA Federal is uniquely positioned to support the needs of government organizations with a cybersecurity strategy that addresses emerging needs and defends against new threat vectors.

"Given that over 300,000 contractors do business with the government, we've prioritized speed-to-market as we know it's top-of-mind for our customers as they migrate to the cloud," said **Kevin Orr, President, RSA Federal**. "We are certified to comply with FIPS 140-2, conform to VPAT accessibility requirements and other standards that are critical to public-sector technology selection. As mandates and requirements continue to evolve, we are committed to supporting federal agencies, public sector organizations and approved federal contractors as they move to the cloud."

Throughout the certification process, SecurID enhanced several core components in its solution that are essential for the federal government, including:

- Cloud Authentication Service (CAS)—A SaaS platform providing single sign-on (SSO) and MFA for SaaS, web and mobile applications.
- Authentication Manager (AM)—AM secures access to on-premises, cloud and web-based applications, verifies authentication requests, and centrally administers policies, users, agents and resources across physical sites.
- Authentication Methods—A broad set of authentication options including award-winning hardware tokens, push to approve, OTP, biometrics, FIDO, SMS and more. Supported by risk-based authentication, the solution uses machine-learning and behavioral analytics for best-in-class identity assurance.
- Agents and APIs—Connectors and standard agents for SAML and RADIUS-based applications, as well as for IIS/Apache, Windows, Unix/Linux and ADFS. In addition, a REST-based API is available to enable MFA for custom applications.