Special Access Programs (SAPs) represent some of the Department of Defense’s (DoD) most sensitive information, and therefore, must be protected accordingly. Reliance upon physical isolation as a primary risk mitigation strategy is no longer sufficient. Threats and risks often outpace the ability to implement robust, multidisciplinary countermeasures. Additionally, costs and timelines to develop new attacks typically pale in comparison to the costs and effort required to implement countermeasures.

Joint Special Access Program Implementation Guide (JSIG) Provides Policy, Procedures and Implementation Guidance

The Joint Special Access Program Implementation Guide (JSIG) serves as a technical supplement to NIST SP 800-53 and CNSSI 1253, and is used in concert with the applicable volume of DoDM 5205.07 in the application of the Risk Management Framework (RMF). JSIG provides standardized cybersecurity/information assurance-related policy, procedures and implementation guidance for managing all networks, systems and system components at all classification levels under the purview of the cognizant SAP Authorizing Official (AO).

Further, the Joint SAP Cybersecurity Working Group (JSCS WG) was established to provide DoD SAP cybersecurity implementation guidance. One key function of the JSCS WG is to promote DoD SAP Community coordination in methodologies for assessing and authorizing SAP information systems and related areas (e.g., documentation, tools, assessment methods and processes).

Tenable Solution Delivers Situational Awareness and Adherence to JSIG Security Controls

SecurityCenter Continuous View® (SecurityCenter CV™) from Tenable is an out-of-the-box solution uniquely positioned to assist in delivering situational awareness to SAP information systems, thus enabling consistency in the measurement, visualization and communication adherence to JSIG security controls. SecurityCenter CV automates the assessment of technical controls from ISO/IEC 27001/27002, the NIST Cybersecurity Framework, JSIG, NIST SP 800-171 and CIS Critical Security Controls to ensure they are in place and operating effectively.

SecurityCenter CV fits JSIG specific needs by supporting “air-gapped” networks, as well as larger enterprise networks. It delivers broad and continuous coverage across physical, virtual, cloud and mobile devices used in IT and industrial control networks. Dynamic asset lists enable you to logically segment, manage and report on the status of specific systems. Intelligent connectors to existing IT and security products audit configurations and analyze events to identify control weaknesses.
SecurityCenter CV Provides Ability to Communicate Security Status

SecurityCenter CV provides fully customizable reports, dashboards and Assurance Report Cards® (ARCs) specific to the leading security frameworks – all out of the box. You can use them “as-is” or easily tailor them to meet your specific security and mission needs. For example, you can easily create specific reports, dashboards and ARCs for individual SAP Programs information systems, as applicable.

The data that SecurityCenter CV gathers and analyzes for security frameworks is often the same data you need for compliance reporting. You can use compliance report templates to present the data in the formats required by multiple compliance standards. As a result, redundant controls are eliminated, and the work required by each audit is reduced.

Tenable reports, dashboards and Assurance Report Cards demonstrate adherence with best practice security controls to external mission partners, as well as large customers that may have the right to audit your security program.

ARCs complement the comprehensive Tenable data collection approach, which uses a combination of active scanning, agent scanning, intelligent connectors to your third-party systems, passive listening and host data monitoring to assess the security posture of your complete infrastructure. Together, these capabilities enable you to:

- Measure, visualize and effectively communicate the technical security controls that help you manage risk
- Communicate security status to internal and external stakeholders
- Understand the context you need to prioritize remediation

About Tenable

Tenable transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable’s customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring by visiting tenable.com.

For more information, visit tenable.com or contact federalsales@tenable.com for a demo.