Ensuring System Protection throughout the Operational Lifecycle

The global cyber landscape is currently occupied with a diversity of security threats, from novice attackers running pre-packaged distributed-denial-of-service scripts to teams of professionals capable of utilizing uniquely obtained zero-days and hidden backdoors to execute advanced persistent threats. Part of the federal response to these actors has been to outline standardized baseline guidance in drivers such as the National Institute of Standards and Technology (NIST) special publications, Federal Information Security Management Act (FISMA), and initiatives like the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program. However, many nuances exist in these drivers and agencies need to interpret and apply them in unique ways based upon organizational, technological, financial, and political concerns, resulting in many agencies struggling to achieve compliance. In fact, the most recent annual FISMA Congressional Report found, "the weakest performances occurred in risk management, continuous monitoring management, contingency planning, and configuration management," with 14 of 22 agencies receiving cybersecurity assessment scores that fell into the yellow and red. For this reason among others, Deltek has predicted that the federal information security market will grow from $7.8 billion in fiscal year 2014 to $10 billion in fiscal year 2019 as agencies engage vendors capable of filling critical knowledge gaps.

Key Federal Drivers

NIST SP 800-53

One of the primary federal drivers, NIST SP 800-53, lays out various controls federal agencies need to implement, grouped by control families, such as:

- Audit and Accountability – Audit and Accountability helps agencies properly define events to be audited, collected, centralized, and reported, as well as the appropriate response to events. Dedicated auditing capabilities and clearly defined incident response plans are essential to properly safeguarding government systems from cyber threats.
- Configuration Management – Configuration Management aims to ensure secure baseline establishment, implementation, monitoring, and reporting. Failure to specify and configure uniform baselines increases the risk of exploitable configurations and the cost of administration and maintenance. Further, it hinders an agency's ability to measure progress in relation to projected costs, deadlines, and performance goals and often leads to unnecessary or inefficient expenditures.

FISMA

FISMA similarly requires agencies to develop, document, and implement cybersecurity programs and a Risk Management Framework for the implementation of security controls, including assistance with the development of Certification and Accreditation (C&A) packages, to include development of System Security Plans (SSPs). Taking this a step further, the Federal Information Security *Modernization* Act of 2014 – an update to FISMA – will replace the antiquated process of annual IT system security checklists with a proactive approach utilizing continuous monitoring.

DHS CDM

Understanding the significant threat level to government networks, Congress established the CDM program run by DHS, and funds the CDM program to support FISMA reporting. With the goal of enhancing agency cyber surveillance capabilities, CDM provides capabilities and tools that continuously monitor, diagnose, mitigate, and repair vulnerabilities. Even with these increased capabilities, individual agencies must establish the reporting and incident response capabilities, processes, and policies to effectively establish a comprehensive security program.

The Tygart Difference

According to the annual FISMA Congressional Reports for FY2013 and FY2014, the number of cyber incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) has increased from 218,886 in fiscal year 2013 to 640,222 in fiscal 2014, an increase of 192 percent. This has resulted in the government moving away from a reactive approach of remediation to a proactive, risk-based approach. It has also highlighted the importance of developing a comprehensive security strategy and implementation program.

As a leading security services provider, Tygart is capable of equipping federal agencies with a comprehensive suite of solutions and core subject matter expertise that allows them to improve their security posture and comply with required standards, all without affecting their ability to complete missions on time and on budget.

Tygart provides agencies a holistic view of their technical configuration through solutions that satisfy control tests and measure compliance. Tygart assesses organizations, to include operational and technical capabilities, and provides recommendations and solutions that not only meet control objectives – but are organizationally feasible and acceptable. Tygart provides technical subject matter expertise for a variety of security-related products, as well as Agency-utilized operating platforms and technologies. Tygart works with agencies to implement requisite continuous monitoring capabilities with the goal of ensuring organizational acceptance of policies, processes, and work instructions.

Tygart's extensive expertise in all aspects of IT Security Management, including Configuration Management, Audit and Accountability, Identification and Authentication, and Continuous Monitoring solutions, improve visibility into security vulnerabilities and identify opportunities for remediation. Tygart provides certified security professionals who partner with executive, management, operational, and technical staff to support the implementation of security initiatives tied directly to agency-specific needs. By balancing existing capabilities and agency goals against known and unknown shortcomings, Tygart is able to provide a comprehensive and tailored security strategy to include the following activities:

Security Assessment and Authorization Readiness

Organizational stovepipes, politics, funding, and contractual obligations or limitations all contribute to an agency's failure to implement effective controls. Tygart eliminates these barriers to effective operation by:

- Working with all stakeholders to identify barriers and root causes to effective control implementation.
- Supporting organizational change management efforts to implement solutions from industry-leading vendors to improve visibility into security vulnerabilities.
- Providing opportunities to remediate vulnerabilities through needs analysis from a security or sustainability perspective for technology solutions or process gaps.
- Identifying control failures, proposing solutions, and conducting market and vendor product analysis.
- Using the Risk Management Framework to identify, prioritize, and recommend strategies for security control implementation.
- Integrating information technologies and improved processes into the organization's standard operating procedures – ensuring demonstrable control compliance.

Configuration Management

Systems often do not have standardized secure configuration baselines, a critical component in achieving even a minimal security posture and for developing additional solutions that address known technological shortcomings. In this capacity, Tygart:

- Provides configuration and change management around the establishment and implementation of secure baseline configurations, while managing the coordination between all involved parties.
- Defines policies, identifies gaps, and then physically implements necessary solutions.
- Tailors secure standard baselines for agency-specific requirements.
- Works with Operations and Maintenance (O&M) teams based on new and improved monitoring to determine non-compliance across devices.
- Coordinates the removal of non-compliant configurations across IT and business units. Infrastructure teams do not always have the comprehensive knowledge about application infrastructure and requirements necessary to comfortably resolve noncompliance.
- Pinpoints specific content within application infrastructures, applies fixes, and then tests each fix in individual environments.
- Applies technology and operating system upgrades to desktops and servers in compliance with implemented baseline standards.

Audit and Accountability

Tygart analysts evaluate policy and processes related to Audit and Accountability to identify gaps and material weaknesses and establish compliant policies and procedures to achieve demonstrably compliant capabilities for all FISMA-defined applications and infrastructure components by:

- Establishing policies that identify the events that require auditing on GSS components and business applications – ensuring compliance with established NIST and FISMA guidance.
- Defining the implementation of auditable events on all IT components – actualizing the policy on IT-specific components.

- Establishing centralized audit repositories for the collection and retention of audit logs.
- Establishing continuous monitoring and incident response capabilities, processes, and artifacts.
- Leading organizational change management activities to socialize new capabilities, processes, and technologies across various organizational units – facilitating the use and expansion of common controls.
- Testing controls, providing artifacts for key milestones.
- Identifying, configuring, and posting artifacts that demonstrate compliance to an auditor.

Risk Assessments – Segregation of Environments

Agencies that share assets between development and operations teams put themselves at risk for insider threat or information mismanagement in organizations where there are inadequate controls to prevent development teams from accessing production systems, applications, and data. Tygart evaluates Information Flow Enforcement and Boundary Protection controls to ensure segregation of environments and identifies comingled development and operational components and dependent processes. Tygart socializes the dependent processes and achieves a consensus on the appropriate resolution to the control failure. That resolution may involve the elimination of the interconnection, if deemed appropriate, or the implementation of compensating controls (firewalls, access control lists, auditing, and supporting review processes). After providing an initial assessment, Tygart begins to implement risk mitigation procedures and solutions, such as:

- Defining the population of developers, operators, production and non-production computer assets, and creating rules for communication between them. Assets are assigned and/or moved to appropriate VLANs (subnets), enabling the enforcement of isolation of servers and workstations; and identifying information flow control parameters such as allowable ports and protocols into guidelines.
- Identifying enterprise assets and communications systems (such as backup systems, intrusion detection systems, monitoring tools, etc.) that need to communicate across environments; and creating and documenting Access Control Lists (ACLs) to ensure organizational identification and acceptance of allowable traffic.
- Creating manageable process and work instructions for the ongoing maintenance of ACLs to enable an agency to continually manage, monitor, and report on information flow controls and parameters.

Risk Assessments – Data Masking

In addition to the (lack of) segregation of environments, standard organizational processes may also compromise the confidentiality of an agency's data, to include Personally Identifiable Information (PII). A common example is if/when an organization refreshes development or test environments with copies of production data – without obfuscating or masking the data in these relatively uncontrolled environments. Tygart evaluates the requirements, processes, and technologies available to limit, if not eliminate, the proliferation of sensitive information – minimizing the risk of intentional and unintentional data breaches. Agencies with a significant developer presence often have an abundance of custom applications and a large number of contractors on development teams. These

factors complicate the ability of an organization to balance authorized access and efficiency of operations with proper security controls. Using state-of-the-art data masking technology, Tygart implements the controls required to ensure no actual PII is used for testing purposes and reduces unauthorized extracts and external distribution. The methods for achieving proper access control include:

- Searching for PII such as social security numbers, names, dates of birth, etc., and performing analysis to validate.
- Using data masking to set up test environments that use data which is structurally identical to the original production data, but has been "masked" so that the actual content is different, thereby protecting PII.
- Establishing new processes that incorporate data masking technologies and techniques to refresh non-production databases.
- Establishing staging areas and data masking templates against those areas, and then using those areas to refresh non-production databases.
- Testing applications in masked environments to minimize the adverse impact on development and support communities, and updating masking algorithms, parameters, and techniques to ensure organizational acceptance as well as control compliance.

Enterprise Patch Management Technologies and Processes

Per NIST 800-40 Rev3, enterprise solutions for continuous patching of information technology components need to be implemented by federal agencies. Often, these patching activities can be readily applied to operating systems and support components. However, the line between General Support Systems (GSS) software components and application components is often blurred – leaving some software components unpatched, or insecurely configured. Often these components are associated with middleware such as application or web server technologies, third-party office support technologies, or even application-specific (COTS, GOTS, or custom) application systems. Tygart is adept at bridging this gap to help an organization "fill the gaps" between application and GSS components. To this end, Tygart:

- Identifies middleware components such as Adobe, Java, Microsoft Office, Apache, and Hadoop, among others. Tygart then proactively manages required coordination between operations staff and application support teams (consumers of web servers, application servers, add-ins, plug-ins, etc.) since operations teams do not always have the level of existing knowledge to comfortably apply patches to middleware without significant coordination with the product consumers.
- Providing timely, updated patches for middleware applications that neither application teams nor infrastructure teams can, or will, unilaterally patch, upgrade, or otherwise remediate. This includes scheduling testing of upgraded applications, establishing secured, patched configurations, and coordinating application re-configurations to become "version agnostic" with regard to middleware components.
- Establishing the capability to incorporate middleware patching activities into standard patching cycles without impact to, or need to coordinate with, business application support personnel or users.

Tygart keeps agencies protected against the latest emerging threats through continual vulnerability patching and scanning to ensure that controls are being efficiently fulfilled and that standard baselines, even those with agency-specific requirements, are maintaining compliance.

Conclusion

In order to implement an effective IT security management program, agencies need to consider the technology, but also the impact the program will have across the agency. Agencies need a partner that can help effectively "fill the gaps" to ensure a comprehensive security posture, including taking into consideration the following:

- Stovepiped organizations
- Internal politics
- Contractual issues
- Lines of responsibility and authority

Agencies need the capabilities and experience offered by Tygart to bridge the development and operations teams, navigate the complex web of agency-specific internal issues and drive organizational assessments and change management programs to ensure mission success.

Contact [marketing@tygart.com] to see how your agency can achieve security and compliance peace of mind.