ATO as Code

Enabling Cybersecurity Modernization Through Risk Management Framework Compliance Automation

Cybersecurity Community of Interest

Date Released: March 26, 2024

Synopsis

This ATO-as-Code report issues a call to action for a unified approach for modernizing the Authorization to Operate (ATO) process or Risk Management Framework (RMF) implementation. This report articulates the significance of intelligent automation in bolstering the efficiency and effectiveness of compliance efforts, thereby enhancing cybersecurity risk management. It underscores the necessity for standardized data communication and advocates for the adoption of Open Security Controls Assessment Language (OSCAL), an open framework for automating assessments.

To that end, the report introduces the Compliance Automation Process Maturity Model (CA PMM), a five-tier framework for organizations to adopt and scale the OSCAL. The report concludes with strategic recommendations for key entities including Congress, the Cybersecurity and Infrastructure Security Agency (CISA), the General Services Administration (GSA), the National Institutes of Standards and Technology (NIST), and other Federal agencies. This work holds significant implications for both cybersecurity experts and policymakers, providing a roadmap for modernizing and automating compliance processes.

American Council for Technology-Industry Advisory Council (ACT-IAC)

The American Council for Technology-Industry Advisory Council (ACT-IAC) is a non-profit educational organization established to accelerate government mission outcomes through collaboration, leadership, and education. ACT-IAC provides a unique, objective, and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT-IAC contributes to better communication between government and industry, collaborative and innovative problem solving, and a more professional and qualified workforce.

The information, conclusions, and recommendations contained in this publication were produced by volunteers from government and industry who share the ACT-IAC vision of a more effective and innovative government. ACT-IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT-IAC collaborative process, refined over forty five years of experience, to produce outcomes that are consensus-based.

To maintain the objectivity and integrity of its collaborative process, ACT-IAC welcomes the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of technology. For additional information, visit the ACT-IAC website at www.actiac.org.

Cybersecurity Community of Interest

The ACT-IAC Cybersecurity Community of Interest mission is to facilitate collaborative development and implementation of solutions and best practices related to cybersecurity challenges. The COI provides opportunities for industry and federal government to identify, raise awareness, and provide solutions to cybersecurity challenges critical to protecting our national interests.

Disclaimer

This document has been prepared to contribute to a more effective, efficient, and innovative government. The information contained in this report is the result of a collaborative process in which several individuals participated. This document does not – nor is it intended to – endorse or recommend any specific technology, product, or vendor. Moreover, the views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable information in this report. However, neither ACT-IAC nor its contributors assume any responsibility for consequences resulting from the use of the information herein.

Copyright

For further information, contact the American Council for Technology-Industry Advisory Council at (703) 208-4800 or www.actiac.org.

Table of Contents

Introduction

The ACT-IAC Cybersecurity Community of Interest convened the Authority To Operate (ATO)-as-Code project team to research the application of automation to increase the efficiency of the compliance process and the effectiveness of cybersecurity risk management. The US Federal government, IT security professionals, and other practitioners involved in the cybersecurity lifecycle are required to adhere to the Federal Information Security Modernization Act of 2014 (FISMA) guidelines. New technologies enable us to automate many currently manual aspects of this process and refocus professionals' time on proactively protecting and securing IT and critical infrastructure.

Objective

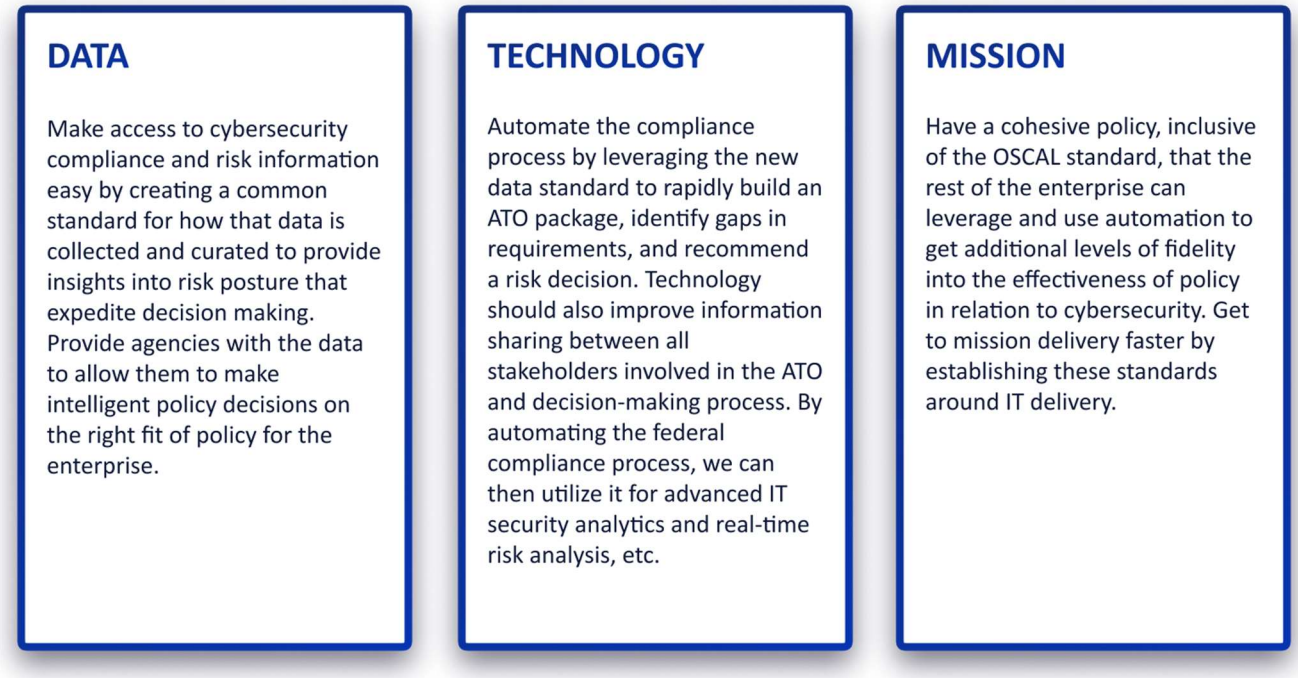
The Federal Information Security Management Act of 2002 (FISMA) harmonized previous legislation (Government Information Security Reform Act, the Computer Security Act of 1987, the Clinger-Cohen Act, and the Paperwork Reduction Act of 1980). In 2014, FISMA was updated, focusing on risk management, continuous monitoring, proactive cybersecurity, and it encouraged agencies to stay up to date on best practices and emerging threats. It is estimated that, since 2002, Federal agencies have spent well over $100 billion to safeguard their IT systems. On paper, FISMA fosters accountability and empowers both agencies and the Office of Management and Budget (OMB) to govern, execute, and enforce the necessary components for implementing a cybersecurity program. Nevertheless, compliance has been slow due to persistent execution and responsibility ambiguities, along with funding constraints since its inception. Compounding the lack of funding with the fact that FISMA has long been viewed as uninspiring and tedious work with no connection to substantive policy goals.

With the increase in security related work, organizations must modernize how to "answer the mail" on the various FISMA requirements. It is our mission to make the compliance process better for IT professionals and their teams that are required to adhere to these guidelines. By reducing manual processes through automation, cybersecurity and IT professionals can focus more on risk management as opposed to the current manual, paper-based processes that *support* risk management. Establishing an industry-standard configuration that is broadly known and well tested will help increase adoption, flexibility and costs associated with the implementation. It is also necessary to identify where data can improve transparency throughout the customer's journey. Data exchange and governance is also vital for the program to integrate with a network of Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Chief Financial Officers (CFOs), and Chief Data Officers (CDOs.)

The ATO-as-Code project team is focused on enabling Federal agencies to transition to a modern cybersecurity compliance and reporting capability that is rooted in the Ongoing Authorizations practice defined in NIST SP 800-53. An efficient and automated Continuous Monitoring (ConMon) Program as defined in NIST SP 800-137 implemented in an automated and streamlined manner is our goal. There are other industry terms like Continuous ATO, that share similar objectives to the ATO-as-Code project objectives.

Critical Success Factors

The ATO-as-Code project team recognizes that a standardized approach to communicating cybersecurity risk data is a prerequisite to begin automating and modernizing the authority to operate process. The driving force behind this project or the critical success factors are:



Business Requirements

To achieve these three critical success factors, the ATO-as-Code project team addressed the following business requirements:

- Use of innovative analytics including threat intelligence to enable real-time risk assessment.
- Collect and analyze quantitative and qualitative data from multiple sources to shape the product roadmap for both internal and external users.
- Lead and facilitate modern agile and DevSecOps practices for the capabilities developed for this effort.

Compliance Automation Process Maturity Model (CA PMM)

On June 10, 2021, the National Institute of Standards and Technology (NIST) released the first version of the Open Security Controls Assessment Language (OSCAL) framework. Since then, OSCAL has gained widespread attention from public and private security leaders. OSCAL provides a standard for capturing and sharing security data to support the compliance life cycle. Although early adopters use OSCAL for assessments, the OSCAL standard can profoundly transform an organization by giving them the ability to measure and automate against enterprise initiatives such as continuous diagnostics and mitigation (CDM), zero trust architecture (ZTA), and continuous authority to operate (C-ATO). Consequently, this project team developed the following process maturity model to assist organizations in adopting and scaling OSCAL. This maturity model requires market advancement of security tools and capabilities.

Process Maturity Model

A process maturity model defines a methodical framework for measuring the effectiveness of an organization's process, such as cyber operations. Additionally, an organization's process can be continuously improved through applying a disciplined methodology, leveraging global standards, and adopting emerging technologies. This model is using OSCAL to power more automation.

The **Compliance Automation Process Maturity Model (CA PMM)** is intended to define a basic model to help organizations safely and rapidly adopt and scale OSCAL. The CA PMM does not prescribe a specific approach to build a fast, high-performing, and security-focused organization, but instead defines the basic principles to measure an organization's process towards that goal. The CA PPM identifies 5 levels of maturity as defined in the sections below.

LEVEL 1: Ad Hoc

Level 1 defines the most basic level where processes are ad hoc, manual, and labor-intensive. In this level, the workforce applies a high degree of manual labor to perform their cybersecurity functions. Also, the workforce may not have a Governance, Risk and Compliance (GRC) tool, or rely on custom GRC platforms, to house security artifacts rather than manage the entire cybersecurity experience. Furthermore, delayed insights about cybersecurity risks hamper decision-making.

#	METRICS	DESCRIPTION
1	Manual creation, editing, and verification of security documents	Organization has a developed enterprise control catalog and creates the System Security Plan (SSP), Security Assessment Plan (SAP), and System Assessment Report (SAR) manually. The process of verifying changes to the documents are also conducted manually.
2	Artifacts are collected in a decentralized manner	Artifacts are collected, edited, and stored in various repositories, tools, or locally.
3	Plans of Actions and Milestones (POAMs) are recorded and tracked manually	POAMs are managed in documents such as a spreadsheet or in a tool that cannot be converted to OSCAL. POAMs are not correlated at the enterprise level.
4	Wet signatures, manual routing	Authorization documents are routed manually and/or signed with wet signature.
5	Reporting is conducted manually	Reports and analytics are generated by teams of people who manually consolidate data sources to provide reports into compliance and risk.

LEVEL 2: Implemented

Level 2 defines the most basic application of the OSCAL framework. In this level, organizations digitize the System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR) and supporting artifacts in the OSCAL standard format[1]. Additionally, organizations in this level rely on commercial GRC platforms that are capable of using OSCAL input and output to digitize and accelerate the security assessment and authorization process, rather than just a repository for security artifacts. Furthermore, organizations leverage OSCAL to automate compliance checks of the security package. However, integration does not yet exist.

#	METRICS	DESCRIPTION

[1]Agencies should analyze and consider using the right OSCAL version such as NIST OSCAL or OSCAL Core to avoid interoperability issues. There are variations in OSCAL implementation e.g. FedRAMP OSCAL.

1	Use OSCAL to digitize the SSP, SAP, and SAR which includes the Organization Baseline and Overlays	Organization stores data in an information system that can ingest the SSP, SAP, and SAR, and export these documents, in OSCAL. Approved leveraged / inherited assets e.g. (Policies, cloud products, other FISMA Systems, etc.) documentation is in OSCAL format.
2	All artifacts and outputs are stored in OSCAL format	Artifacts (anything that is system-generated that proves the security compliance of a system) are stored in a digital format and in a manner where they can be easily retrieved by an organization / structurally retrieved, considering multiple storage methods (E.g., S3 storage, DB, log aggregator). The organization is now accepting digitized versions as part of their OSCAL assessments.
3	Automated POAM Generation	POAMs are automatically generated based on finding / vulnerability age, and notification of reminders are provided to track and remediate POAMs.
4	Automated routing of approval & digital signatures	Packages are automatically routed, and digital signatures are applied. Reduce overall approval processing time due to automated routing and convenience of digital signature capability.
5	Automated reporting and analytics	Reports are generated automatically and enable the organization to trend metrics (e.g., findings, remediation, and risk over time. These metrics are further used to identify aggregated metrics like throughput of findings and remediation coverage.)
6	Ongoing Authorization with Some Manual Attestation	Systems are mature and undergo check-ins and due diligence on a scheduled basis and are still subject to periodic manual reassessment.

LEVEL 3: Integrated

Level 3 defines the level where the organizational processes are interconnected with external and internal processes. For example, the organization's security assessment and authorization processes are interconnected with the Federal Risk and Authorization Management Program (FedRAMP) process. Additionally, control compliance, overlays, and inheritance are seamlessly shared between

the organization and governing bodies. Organizations in this level often rely on OSCAL to not only automate security artifact generation, but also transmit security events from CDM platforms. Here, organizations begin to integrate security management activity that will flow into the compliance process (e.g., patch management, asset tracking and reporting, etc.). These are interconnected and insights from these platforms are displayed in centralized dashboards. Organizations establish Open application programming interface (APIs) to interconnect systems and enterprise Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) to centralize the management of key technologies.

#	METRICS	DESCRIPTION
1	Organization Provides Enterprise Capabilities and Software in Preapproved Format with Leveraged Controls the Software Provides	All templates are in OSCAL format, and the organization can pull information into that template. Implementation statements for enterprise common control catalog are pre-populated in these templates. All inherited assets and artifacts are collected in an OSCAL format and can be leveraged to identify asset-level and leveraged-risk. For example, policies, FedRAMP products, etc.
2	Security Compliance Baseline Information is Integrated into the Compliance Process	System security posture, compliance scans, and other important information that is used to manage the system life cycle is automatically collected, tagged, and integrated into the compliance process and activities.
3	Compliance information is automatically published to relying parties	Organization has integration with relying parties to provide compliance information in an automated way, such as Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), industry partners, etc.
4	Alert-Based Ongoing Authorization	Systems are mature based on established enterprise criteria (e.g., integration with CDM) and undergo check-ins and due diligence based on automatically generated alerts. OSCAL-formatted data provides a near real-time assessment of risk posture which is provided in a dashboard view to track and prioritize activities.

LEVEL 4: Measured

Level 4 defines the level where cybersecurity risk, budget, and mission alignment are measured, quantified, and embedded into executive decision-making. Here, the business organization, technology organization, and cyber operations are aligned and working in tandem to properly manage risk without impeding the mission. Organizations in this level rely on an enterprise risk framework that strategically embeds cybersecurity into the organization's scorecard. Enterprise governance is established to manage the business-technology-security alignment. Enterprise management platforms for planning, budget, and acquisitions are more integrated with cybersecurity platforms by using OSCAL.

#	METRICS	DESCRIPTION
1	Integration with the Business and Acquisition Tools	Business, acquisition, budget, cyber, and IT operations are integrated. POAMs tie in the cost to remediate.
2	Performance Benchmarking Across Teams & Organizations	Performance is compared across teams to benchmark cybersecurity performance across teams and organizations. Success metrics are collected to track success of the OSCAL program.
3	Assess risk across all Infrastructure Types	Software Bill of Materials (SBOM), Cloud, and Container information is integrated with overall risk to address risk down to the container level. OSCAL tags are applied to data to integrate this data into overall compliance.
4	Live Dashboards with Risk Information	Reports include business-level risk, in addition to system-level risk, which are updated in real time.

LEVEL 5: Automated and Optimized

Level 5 defines the highest level in the process maturity model where the organizational processes are continuously digitized, integrated, measured, and automated all using OSCAL. Additionally, organizations at this level can use extreme automation to learn, adapt, and optimize business processes. They also leverage a degree of intelligent automation like artificial intelligence to predict risk and protect the organization. This level requires the greatest degree of organizational change. The workforce and culture must appreciate and embrace data to power not only cyber security strategy, but also its operation.

#	METRICS	DESCRIPTION
1	Continuous ATO (C-ATO)	The data arising from changes in your FISMA boundary drives and informs the decision making. Recommendations, stage gates, etc. before going to production to make a risk decision. Auto-approval is possible based on the identified risk and findings.
2	Intelligently Predict System Risk	The organization can predict risk based on past and present data by using artificial intelligence (AI).
3	Identify Risk Based on Collective Intelligence Across all Systems	Generate an SSP with the exact posture of that system and calculate the risk based on the aggregation of all those results. Intelligence is consolidated across all systems and leveraged to detect risk with other systems.
4	Automated Data Call Responses	Since all data is consolidated in a central repository, data calls can be responded to by selecting the requirements of the requestor. Based on a change in the system reflected in the data, you raise the risk that becomes something you must address. Leverage information on system behavior.
5	Policy as Code	Automatically update requirements based on the changes in policy. Automate zero trust checks for system changes.

Recommendations: Compliance Automation Federal Jumpstart

The **Compliance Automation Federal Jumpstart Guide** provides the final and most important chapter in the series because it identifies a structural flaw in current cybersecurity operations and recommends a whole-of-government approach to curing this flaw. The Federal government has traditionally delegated the responsibility of protecting critical systems to each Federal agency. Additionally, funding has been disproportionately divided between serving the mission and securing the information systems that deliver that mission. While standards were enacted centrally, decentralizing the fight against sophisticated bad actors does not allow us to unleash the full might and power of the Federal government.

Bad actors will use any and all means to infiltrate our critical information systems, leveraging artificial intelligence for uncovering weaknesses in our infrastructure and deep fakes for social engineering. They will simultaneously attack our infrastructure at different points and take advantage of our inability to act as one unified Federal government. The only way to protect against this is to rethink our conventional wisdom. For example, we have traditionally limited sharing data between the public and private sectors, making it impossible for the private sector to build AI to fight back. Ironically, bad actors that have already hacked into our information systems may have more of our data than good actors that have the powerful technology to protect us.

The paper identified a few essential bodies that must work in concert to lay the foundation for a whole-of-government approach to cybersecurity:

(1) Congress;
(2) Cybersecurity and Infrastructure Security Agency (CISA);
(3) General Services Administration (GSA);
(4) National Institutes of Standards and Technology (NIST); and
(5) Federal Agencies.

Congress

Congress has appropriated many powerful laws to protect our national and critical information systems such as the National Security Act (1947); Health Insurance Portability and Accountability Act (HIPAA) (1996); Gramm-Leach-Bliley Act (1999); Homeland Security Act (2002); Federal Information Security Management Act (FISMA) (2002); Federal Risk and Authorization Management Program (FedRAMP); Federal Information Security Modernization Act (2014) and Cyber Incident Reporting for Critical Infrastructure Act (2022). While these laws provide a powerful framework, Congress has not sufficiently funded Federal agencies so that they can properly execute these laws. Instead, Federal agencies, with limited budgets, are forced to implement partial solutions that are neither fully nor intelligently automated.

Provide Funding for Intelligent Automation of Cybersecurity

Federal agencies face budget cuts in the coming years making it nearly impossible for them to procure modern cybersecurity platforms. Congress must assist by providing funds to modernize governance, risk and compliance platforms and the integration of those platforms with software agents running on services and edge devices.

Cybersecurity and Infrastructure Security Agency (CISA)

Enabled by the amended Homeland Security Act of 2002, the Cybersecurity and Infrastructure Security Agency (CISA) tracks cybersecurity risk by collecting and analyzing cybersecurity data from Federal Agencies. The process to collect this data is often labor-intensive, not standardized, and subjected to delays. CISA could make a few strategic investments to modernize the process and proactively respond to modern threats.

- **Build a Domain-Specific Marketplace for Cybersecurity Data**
  Cybersecurity threats may vary by domain such as healthcare, finance, national security, and critical infrastructure. Consequently, CISA could build a domain-specific data marketplace for cybersecurity data. Federal agencies can contribute data to and mine the data in the marketplace to uncover risks and threats.
- **Deidentify Data and Make It Accessible to Cleared Companies**
  CISA can deidentify the data and make it available to commercial companies. Commercial companies can build Advanced AI, at their own cost, to detect anomalies, identify vulnerabilities, and recommend offensive and defensive measures. Companies can license the insights to Federal agencies, who can select from the best commercial model. By shifting the cost to the private sector, Federal agencies can simultaneously reduce the cost and increase the quality of the predictions. Commercial companies must compete based on outcome and price without facing complex procurement regulations.

- **Create Centralized and Open Risk Registry for Cybersecurity Threats**
  CISA can also create a centralized and open risk registry for anyone to share cybersecurity threats indexed by a uniform code.

General Services Administration (GSA)

The General Services Administration (GSA) is charged with the responsibility of accrediting all cloud products sold to the Federal government. With demand increasing rapidly, GSA has already started the process of automating the accreditation process using OSCAL. The OSCAL standard can profoundly address the foundational data flaw, if and only if, the standard becomes pervasive.

- **Promote Widespread OSCAL Adoption in the Federal Government**
  Federal agencies have not yet adopted OSCAL and many still rely on legacy GRC platforms that are not OSCAL-compliant. However, GSA is perfectly positioned to incentivize Federal Agencies to accelerate their adoption of OSCAL. GSA can create a curated, intelligent, and centralized OSCAL repository for IaaS, PaaS, and SaaS. GSA can open the repository to Federal agencies only if they have GRC platforms that can process OSCAL. In order to ensure the interoperability goals from the use of OSCAL, GSA should explore ways of developing an OSCAL Component Definition repositories for cloud services and software products which can be used government-wide.
- **Continue to Automate Access to FEDRAMP Security Data**
  GSA can extend the ecosystem by allowing Federal agencies to "leverage" security artifacts and inherit IaaS, PaaS, and SaaS common controls. Federal Agency Governance, Risk, and Compliance platforms can directly link to the GSA OSCAL repo to create an integrated, data fabric linking applications to platforms to infrastructure.
- **Require All Software Vendors to be OSCAL-Compliant Using a Standardized Version of NIST OSCAL or OSCAL Core.**
  GSA can require all vendors selling cloud products to the Federal government to create and submit the security package using OSCAL so that everyone is working under one uniform data standard.

National Institutes of Standards and Technology (NIST)

The National Institutes of Standards and Technology (NIST) is charged with the responsibility of defining and promoting critical industry standards and frameworks. The NIST Cybersecurity Framework (CSF), RMF, and OSCAL are essential frameworks and standards for cybersecurity.

- **Make OSCAL Flexible So That It Can Support Unique Needs of Federal Agencies**
  OSCAL defines a standard data model and referential structure for the system security plan, component inventory, plan of action and milestones, security assessment plan, and security assessment report. A validator (schematron) has been built to check the integrity of security packages submitted using OSCAL. The validator is extremely useful but is somewhat restrictive. Relaxing the restrictions could accelerate the adoption of OSCAL by Federal agencies.
- **Extend OSCAL from Assessment to Continuous Monitoring**

OSCAL has the power to revolutionize cybersecurity, but so far OSCAL is only limited to governance, risk, and compliance. Extending OSCAL to continuous diagnostics and mitigation could profoundly change the dynamics of cyber ops as a whole. NIST could define the standard data model and referential structures for security information and event management (SIEM) and CDM platforms so that data about vulnerabilities, incidents and risks can be shared in a standardized fashion.

- **Define Standard APIs for Cybersecurity Products**
  As far as we know, NIST has not defined a set of standard APIs for cybersecurity. As cyber-attacks intensify, Federal agencies will need to create a more integrated defensive ecosystem powered by Open APIs. Vendors supplying cyber platforms with Open APIs could radically change the way we identify, detect, protect, detect, respond, and recover from security incidents.

Federal Agencies

Federal Agencies have been fighting adversaries with legacy technologies but that is about to change. Through ACT-IAC, public and private sectors have come together to promote standards, enhance products, and introduce innovative new ways to fight back. The section below describes ways in which Federal agencies can take advantage of the emerging tools.

- **Embrace OSCAL-Native Governance, Risk, and Compliance Platform**
  Emerging vendors are introducing OSCAL-native capabilities to help Federal agencies automate manual/labor-intensive processes. Vendors of GRC platforms are the first to embrace OSCAL. Federal agencies should reevaluate their legacy platforms and plan to modernize legacy processes and platforms.
- **Establish Cybersecurity Data Governance and Practice**
  Federal agencies should establish data strategy, governance, and practice for cybersecurity and shift the culture from a human-based system to a human-machine based system. Using a data-centric model, Federal agencies can rapidly augment human intelligence with 24x7 machine intelligence to detect vulnerabilities and protect critical information systems.
- **Facilitate a Rapid Mechanism for Buying Cyber Security Innovation**
  The cybersecurity industry is constantly evolving as adversaries leverage whatever means necessary to access our critical information systems. Consequently, combating creative and sophisticated adversaries requires an innovative ecosystem that is adaptable. Federal agencies must put in place dynamic acquisitions to streamline the procurement of cyber innovation through cloud subscriptions. Federal agencies must be able to swiftly switch from one vendor to another. Vendors must constantly compete by providing superior products.

Authors & Affiliations

This white paper was written by a consortium of government and industry. The organizational affiliations of these contributors are included for information purposes only. The views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development.

Daniel Jacobs	Office of Personnel Management
Gaurav “GP” Pal	stackArmor
Paul Weston	U.S. Immigration and Customs Enforcement
Satyaveer Satvat	General Services Administration
Macey Smith	US AI
David Nguyen	US AI
Rachel Sile	Department of the Interior
Dr. Prentice Norman	VMD Corp.
Pirooz Javan	Easy Dynamics Corp
Janis Richards	Gunnison Consulting Group, Inc.
Marcus Walker	ASRC Federal
Jamal Webster	CGI Federal
H. Ahsan	TechIcon, Inc