ACT-IAC  
ATO-AS-CODE

Compliance Automation Federal Jumpstart

Version 1.0  
September 30, 2023

# INTRODUCTION

On September 30, 2023, the ACT-IAC ATO-AS-CODE working group published the (1) Compliance Automation Business Case; (2) Compliance Automation Process Maturity Model (CA PPM); and (3) Compliance Automation Federal Jumpstart Guide with the goal of helping Federal Agencies intelligently automate cyber operations to protect critical information systems from foreign and domestic threats.

The Compliance Automation Federal Jumpstart Guide (this document) 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 such artificial intelligence for uncovering weaknesses in our infrastructure and deepfakes 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.

We have identified a few essential bodies that must work in concert to lay the foundation to jumpstart the 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); 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 year, making it nearly impossible for them to buy modern cybersecurity platforms. Congress can 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.

# CISA

Enabled by the Homeland Security Act, 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 can 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 can 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. A few examples include Root cause analysis, after action reports and relevant security logs. With generative AI the unstructured data combined with the structured security logs could be used to predict the likelihood of future events.

## 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.

# 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 Governance, Risk and Compliance 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 up the repository to Federal Agencies only if they have GRC platforms that can process OSCAL using FedRAMP as an example.

## 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

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.

# 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 CSF, RMF, and OSCAL are essential frameworks and standards for cybersecurity.

## MAKE OSCAL FLEXIBLE SO THAT IT CAN SUPPORT UNIQUE NEEDS OF FEDERAL AGENCIES

The Open Security Controls Assessment Language (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 can accelerate the adoption of OSCAL by Federal Agencies.

## EXTEND OSCAL FROM ASSESSMENT TO CONTINUOUS MONITORING

The Open Security Controls Assessment Language (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 can profoundly change the dynamics of cyber ops as a whole. NIST can define the standard data model and referential structures for 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 application programming interfaces (APIs) for cybersecurity. As the 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 can radically change the way we identify, detect, protect, 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, the 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 labor-intensive processes. Vendors of governance, risk and compliance platforms are the first to embrace OSCAL. Federal Agencies should reevaluate its 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

Unlike any other industry, the cyber industry is constantly evolving as adversaries leverage whatever means necessary to access our critical information systems. Consequently, combating creative and sophisticated adversaries requires an innovation ecosystem that is adaptable and standardized. Federal Agencies can 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 ensuring they are leveraging the most optimal solution for their mission needs while minimizing risk. Vendors must constantly compete by providing superior products.