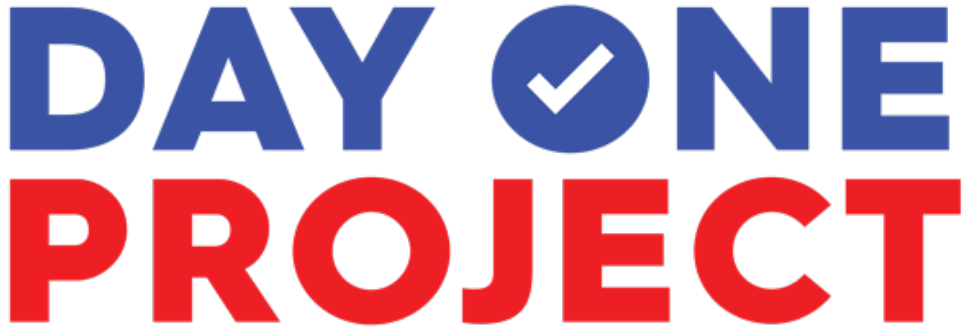

Compliance as Code and Improving the ATO Process

Mary Lazzeri
Dayton Williams
Greg Elin
Fen Labalme

January 2021

Summary

A wide-scale cyber-attack in 2020 impacted a staggering number of federal agencies, including the agency that oversees the United States nuclear weapons arsenal. Government officials are still determining what information the hackers may have accessed, and what they might do with it.

The fundamental failure of federal technology security is the costly expenditure of time and resources on processes that do not make our systems more secure. Our muddled compliance activities allow insecure legacy systems to operate longer, increasing the risk of cyber intrusions and other system meltdowns. The vulnerabilities introduced by these lengthy processes have grave consequences for the nation at large.

In federal technology, the approval to launch a new Information Technology (IT) system is known as an Authority to Operate (ATO). In its current state, the process of obtaining an ATO is resource-intensive, time-consuming, and highly cumbersome. The next administration should kick-start a series of immediate, action-oriented initiatives to incentivize and operationalize the automation of ATO processes (also known as "compliance as code") and position agencies to modernize technology risk management as a whole.

Challenge and Opportunity

While the compliance methodologies that currently comprise the ATO process contribute to managing security and risk, the process itself causes delays to the release of new systems. This perpetuates risk by extending the use of legacy—but often less secure—systems and mires agencies with outdated, inefficient workflows.

To receive an ATO, government product owners across different agencies are required to demonstrate compliance with similar standards and controls, but the process of providing statements of compliance or "System Security Plans" (SSPs) is redundant and siloed. In addition, SSPs are often hundreds of pages long and oriented toward one-time generation of compliance paperwork over an outdated, three-year life cycle. There are few examples of IT system reciprocity or authorization partnerships between federal agencies, and many are reluctant to share their SSPs with sister organizations that are pushing similar or even identical IT systems through their respective ATO processes. This siloed approach results in duplicative assessments and redundancies that further delay progress.

The next administration should shift from static compliance to agile security risk management that meets the challenges of the ever-changing threat landscape. The following Plan of Action advances that goal through specific directives for the Office of Management and Budget (OMB)

Office of the Federal CIO (OFCIO), General Services Administration (GSA), Technology Transformation Service (TTS), and other agencies.

Plan of Action

The Office of Federal Chief Information Officer (OFCIO) should serve as the catalyst of several of activities aimed at addressing inefficiencies in the ATO attainment process.

Action One: OFCIO should draft an OMB Compliance as Code Memorandum that initiates two major activities.

First, the Memorandum will direct GSA to create a Center of Excellence within the Technology Transformation Service (TTS). The goals and actions of the Center of Excellence are detailed under "Action Two" below.

Second, the Memorandum should require Cabinet-level agencies to draft brief "exploration and implementation plans" that describe how the agency or agencies might explore and adopt compliance as code to create efficiencies and reduce burden.[1]

OFCIO should offer guidance for the types of explorations that agencies might consider. These might include:

- The integration of development, security and operations (DevSecOps)[2] in major systems to allow for the automated validation of security controls.
- The identification of a pilot system or application within each agency that can be leveraged for the conversion of SSPs into a machine-readable format that allows for experimentation with compliance automation.
- The appointment of a single, accountable leader within each agency to guide and oversee compliance as code explorations as well as provide regular reporting to agency Chief Information Officers.

During the plan review process, the OFCIO should collaborate with the Resource Management Offices (RMOs) at OMB to identify agencies that offer the most effective plans and innovations.[3] Finally, OFCIO should consider releasing a portion of the agency plans publicly with the goal of spurring research and collaboration with industry.

[1] We suggest the following timeline: By June of 2021 agencies will develop and submit their plans to OFCIO for review. OFCIO will collaborate with agencies, revise and ultimately approve plans by December of 2021. Plan implementation would begin in 2022.

[2] DevSecOps requires the integration of infrastructure security throughout an agile development lifecycle. The term DevSecOps was coined to emphasize the need to build security gates and protocols into DevOps projects.

[3] The OMB Technology Modernization Fund could be leveraged to fund promising pilot projects within agencies. Those pilots can be overseen and aided by the newly created GSA Center of Excellence.

Action Two: The General Services Administration should create a Cybersecurity Compliance Center of Excellence.

OMB should commission the creation of a Cybersecurity Compliance Center of Excellence at the General Services Administration (GSA). Joining the six other Centers of Excellence, the Cybersecurity Compliance Center of Excellence (CCCE) would serve to accelerate the adoption of compliance as code solutions, analyze current compliance processes and artifacts, and facilitate cross-agency knowledge-sharing of cybersecurity compliance best practices. In addition, OMB should direct GSA to establish a Steering Committee representative of the Federal Government that leverages the expertise of agency Chief Information Security Officers (CISOs), Deputy CISOs, and Chief Data Officers (CDOs) as well as representatives from the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

The CCCE Steering Committee will research potential paths to propagate compliance as code that are not overly burdensome to agencies, deliberate on these initiatives, and guide and oversee agency innovations. The ultimate goal for the Steering Committee will be to devise a strategy and series of practices to increase compliance as code adoption via the Cybersecurity Compliance Center of Excellence and OMB oversight.

The following sections detail potential opportunities for CCCE Steering Committee investigation and evaluation:

- Study IT System Acquisition Rules for Vendor Compliance Information.

  The Steering Committee should review existing acquisition guidance and consider drafting a new acquisition rule that would require software vendors to provide ATO-relevant, machine-readable compliance information to customer agencies. The data package could include control implementation statements, attestation data and evidence guidance for the relevant NIST controls.[4] In addition, the new system and process improvements should be agile enough to allow the incorporation of controls unique to a particular application or service.

  Shifting the responsibility of managing compliance information from agencies to vendors saves time and taxpayer dollars spent in the duplicative discovery, creation, and maintenance of control implementation guidance for common software. The rule would be doubly effective in time saved if the vendor's compliance data package has common reciprocity between agencies, allowing for faster adoption of software government wide.[5] Finally, the format of the data package should be open sourced, fungible and accessible.

[4] The reference code for this evidence collection and verification should be open sourced and in a publicly available (e.g. GitHub) repository so that it can be easily reviewed for security by the compliance community.

[5] Regarding a proposed new acquisition rule for vendor compliance data, OMB should consider exemptions for acquisitions below a certain dollar value. Larger software providers can more easily meet the technical and logistical requirements of this rule, whereas

- Examine and Improve the Utility of System Security Plans (SSPs).

System Security Plans are the baseline validator of a system's security compliance and a comprehensive summary of an IT system's security details.[6] OMB and the CCCE Steering Committee should direct agencies to investigate the reusability and transmutability of System Security Plans (SSPs) across the Federal Government. A research-focused task force, composed of federal data scientists, compliance subject matter experts, auditors, and CISOs, should research how SSPs are utilized and draft recommendations on how best to improve their utility. The research task force would collect a percentage of agency SSPs, compare time-to-ATOs for various government organizations, and develop a common taxonomy that will allow for reciprocity between government agencies.

- Create a Federal Compliance Library.

The Steering Committee should investigate the creation of an inter-agency Federal Compliance Library. The library, most likely hosted by NIST, would support cross-agency compliance efforts by offering vetted pre-sets, templates, and baselines for various IT systems. A Federal Compliance Library accelerates the creation and sharing of compliance documentation and allows for historical knowledge and best practices to have impact beyond one agency. These common resources would free up agency compliance resources to focus on authorization materials that require novel documentation.

- Explore Open Security Controls Assessment Language (OSCAL).

The Steering Committee should explore the value added by mandating the conversion of agency SSP components to machine readable code such as Open Security Controls Assessment Language (OSCAL).[7] OSCAL allows for the automated monitoring of control implementation effectiveness while making documentation updates easier and more efficient.

Conclusion

Federal compliance processes are ripe for innovation. The current system is costly and perpetuates risk while trying to control for it. The Plan of Action detailed above creates a cross-agency collaborative environment that will spur localized innovations which can be tested and perfected before scaling government wide.

---

smaller firms may not have such resources at hand. Small businesses should receive support from the agency Small Business Offices or GSA to produce the material in the appropriate format.

[6] Validators, extensions and shift-left DevOps hooks provide an equivalent resource.

[7] OSCAL, currently being developed by NIST, is a "set of hierarchical, formatted, XML- and JSON-based formats that provide a standardized representation for different categories of information pertaining to the publication, implementation, and assessment of security controls" See: Open Security Controls Assessment Language, NIST https://csrc.nist.gov/Projects/Open-Security-Controls-Assessment-Language#:~:text=NIST%20is%20developing%20the%20Open,and%20assessment%20of%20security%20controls.

Frequently Asked Questions

1. Why is this recommendation important?

Current compliance processes are slow, costly and ineffective. They result in bureaucratic inertia that stalls the adoption of new technologies and exacerbates risk. The compliance-as-code recommendations outlined in this text dovetail with conclusions drawn from the Federal Cybersecurity Risk Determination Report and Action Plan to the President of the United States (2018). Compliance-as-code solutions match core actions that are necessary to address cybersecurity risks across the federal enterprise.[8]

2. Why are OFCIO and TTS best positioned to lead these efforts?

OFCIO and TTS have been successful in guiding and monitoring agencies through a number of technology transformation initiatives including Data Center Consolidation Initiative[9], the HTTPS-Only Standard[10], and the FITARA Scorecard[11] among many others. OMB OFCIO has the ability to direct agencies to develop exploration plans, as described above, and GSA TTS is well situated to stand up a new Center of Excellence to facilitate pilot initiatives and cross-agency collaboration. In addition, a Steering Committee for the Cybersecurity Compliance Center of Excellence (CCCE) that leverages the expertise of CISOs, Deputy CISOs, and CDOs as well as representatives from NIST and DHS CISA can ensure that GSA and OMB are developing guidance based on the actual situations within agencies. Greater participation and representation from agencies will ensure greater transparency, collaboration and adoption of new innovations.

3. How will these proposals make the ATO compliance process more efficient?

ATO processes have been a known encumbrance for some time. A handful of agencies have begun to explore automation and compliance as code, including, but not limited to, the Defense Digital Service Rapid ATO[12] and the Centers for Medicare and Medicaid "Simplified and Guided Authorization for Rapid ATO" pilot. While many agencies recognize the need, most lack the resources to explore innovations and automate processes. These proposals aim to elevate the issue and proposed solutions to the White House level and align the most promising innovations with support and funding. Once solutions are identified and tested, they can be scaled for government-wide adoption.

---

[8] Specifically, these actions are: (1) standardize IT and cybersecurity capabilities to control costs and improve asset management, and (2) drive accountability across agencies through improved governance processes, recurring risk assessments, and OMB engagement with agency leadership.

[9] Data Center Consolidation Initiative. https://www.gsa.gov/technology/government-it-initiatives/data-center-optimization-initiative-dcoi.

[10] HTTPS-Only Standard. https://https.cio.gov/.

[11] FITARA Scorecard. https://management.cio.gov/.

[12] Defense Digital Service Rapid ATO. https://dds.mil/work/tech-navigators

4. Are there risks to centralizing all IT compliance in one library? Are there security concerns?

Published data formats provide greater security than proprietary counterparts. While the reference implementations and data formats must be open, the data collection and analysis of an operational system is fully protected by encryption. If required, certain SSPs can be delivered to new agencies on a by-request basis instead of being made publicly available.

5. Is it overly burdensome to ask agencies to convert their SSPs to OSCAL?

OSCAL integration across the Federal Fovernment should be evaluated for burden and agencies' current technical capacity to support OSCAL integration must be considered. Agencies should consider smaller-scale integrations of OSCAL as a starting point. Research should also be focused on potential time saved from automating compliance checks, streamlining the review process, and increasing the speed of adopting new technologies.

6. Are there any legal requirements or obstacles for agencies that may prevent them from participating in these reforms?

The request that software vendors provide machine-readable security documentation is to their own benefit. It is currently cumbersome and repetitive for a software vendor to provide information to support the ATO process on an individual basis every time their software is evaluated or implemented. Vendors already decide what information to share and are likely careful about what they choose to provide. A shared SSP library or reciprocity of SSP statements across agencies should not introduce any new legal obstacles or concerns into the process. Vendors should be made aware that any information they share is eligible for a cross-agency shared repository.

7. What exactly is the scope of the term "compliance as code"? in technical terms?

'Compliance as Code' is the automated implementation, verification, remediation, monitoring and reporting of compliance information and status. In technical terms, compliance as code can be facilitated by migrating the static SSP from Microsoft Word to OSCAL, including front matter, control implementation statements, and appendices. Additional examples of compliance as code include: evidence gathering and verification code, commit and pull-request automated testing, and DevOps context aware notifications and documentation. Developer tools such as an RMF and OSCAL-Aware GRC plugin for VS Code and continuous monitoring plugins can also be included.

About the Authors

Mary Lazzeri is the Federal Strategy Director at CivicActions. She served as a technology advisor for the Office of Management and Budget and the United States Digital Service under the Obama Administration. She has led digital transformation initiatives across the Federal Government and has co-authored federal security, privacy and cloud policies.

Dayton Williams is an Associate Developer and Policy Lead at GovReady PBC. Mr. Williams has supported GovReady PBC's compliance initiatives in various federal agencies and specializes in RMF compliance automation.

Greg Elin is the Founder and CEO of GovReady PBC, a company focused on shifting cybersecurity and compliance left in the System Development Life Cycle. Mr. Elin was previously the Chief Data Officer for the Federal Communications Commission where he established trends for open data, APIs and the role of CDOs in federal agencies. He is currently working with DHS, CMS, USDA, and others on compliance automation.

Fen Labalme is the Chief Information Security Officer at CivicActions. His current mission is to empower better government by delivering free and open source software (FOSS) security and compliance solutions that improve upon previous proprietary systems. He's also working on automating the ATO process, making it easier for agencies to do business securely. Fen is a long-time advocate of handling information wisely. His Computer Science and Electrical Engineering thesis at MIT presaged the privacy concerns facing today's Internet and social media platforms.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of the next presidential term. For more about the Day One Project, visit **dayoneproject.org**.