RECREATION.gov
BRING HOME A STORY

RECREATION.GOV RECEIVED THE ATO IN 2019.

Here's How It Can Help You.

WHAT IS AN ATO AND WHY DOES IT MATTER?

The Federal Information Security Management Act (FISMA), passed in 2002, requires federal agencies to develop, document, and implement information security plans to protect sensitive data. All systems transmitting, storing, or processing data that belongs to the federal government are subject to FISMA standards and are required to have an Authority to Operate (ATO) regardless of who owns the infrastructure or application. An ATO assesses the management, operational, and technical security controls within a system. Systems that handle federal data without an ATO are not considered compliant. Agency CIOs may shut down systems operating without an ATO or defund their associated programs. System Owners of noncompliant systems may receive negative performance appraisals or be subject to disciplinary actions. Agencies who do not report on and meet FISMA compliance may lose funding from OMB, and individuals responsible for noncompliant system may be subject to disciplinary action, including termination. In the event of a breach, the Agency will likely be responsible for notifying the impacted individuals and providing credit monitoring services.

RECREATION.GOV: THE JOURNEY TO ATO

For Recreation.gov, securing data was critical due to the nature of this program and the data that it handles. As the official source for travel ideas, trip planning, and booking reservations across America's federal lands, waterways, and monuments, the Recreation.gov platform hosts nearly 20 million user sessions each year. Federal public land and water managers across 3,500 recreation areas use the platform for daily operations including communicating with visitors and other staff, financial collections, and accessing a variety of reports that help track visitation and identify trends.

LAYING THE FOUNDATION

Booz Allen Hamilton, the developer of the new Recreation.gov platform, brought strong expertise in building secure and compliant solutions for business systems governed by FISMA requirements. Long before the process of securing an ATO began, the Recreation.gov team had designed and implemented architecture, tools and processes to ensure a secure system. This deliberate approach helped make the ATO process a success.

From the beginning, processes were defined for creating and deploying changes to the environment, security impact assessments were conducted, minimum password length and complexity guidelines were established, and well-defined roles implemented "least privilege", providing access to only the things each stakeholder needed. Network security tools including a firewall to monitor incoming and outgoing traffic, antivirus technology, data encryption products, log aggregation, and account management functionality were embedded into system architecture. Vulnerability scanning tools continually search through the platform's infrastructure to find things that aren't patched or could be footholds for intruders.

LAYING THE FOUNDATION (CONTINUED)

Recreation.gov servers are also physically secured and access is monitored and controlled. In addition, the system applied appropriate network segmentation during development. This precaution proved important during the ATO process because if a system applying for an ATO resides on a network with other systems, each must undergo the ATO process. Any resulting changes required can be complex and time-consuming. All of these things took place before the long road to applying for and achieving the ATO.

THE AUTHORIZATION PROCESS

The ATO process can be extensive, lengthy and expensive. Systems with an ATO must staff an Information System Security Officer (ISSO) to support the Risk Management Framework (RMF) lifecycle. ATO applicants must prepare a significant amount of documentation for evaluation, including a system security plan, privacy threshold analysis, a configuration management plan, incident response plan, and a contingency plan, among others. Technology providers that are unfamiliar with the process face a steep learning curve and may need to make significant investments in time and resources to improve security and to navigate the process. The government will review all materials to ensure they meet the FISMA requirements from their perspective. ATO requirements vary by agency, so there is no "one-size-fits-all" approach for the process. Once there is alignment on the documentation, a third party assessment organization will validate that each of the requirements has been met across the system. Deviations are scrutinized, analyzed, and resolved. The ATO requires monthly maintenance activities until the next annual audit. System changes must be reviewed and approved by the ISSO to evaluate impact to existing security controls. System changes include everything from what type of data is in the system, who has access to which data and features, and technical details like how a particular function is implemented what software versions are used.

The comprehensive security designed and built into the new Recreation.gov platform helped reduce the time it took to complete the ATO process. Even with the actual design and implementation work completed, the ATO process took close to a year and several hundred thousand dollars to complete. Every change that is made to the system is assessed to determine if there is an impact to the ATO. There is also an annual review of the security systems that ensures the program remains compliant with all requirements within the ATO. Navigating the comprehensive ATO requirements, walking through each line of code to ensure the system met the underlying controls, writing documentation for each control, implementing additional controls, and keeping the documentation up to date is not a small effort.

RECREATION.GOV HELPS FACILITIES SAVE TIME AND RESOURCES

Recreation.gov received its ATO in 2019 and continually monitors various control elements through Plans of Action and Milestones (POAMs). With its ATO in place, Recreation.gov enables agencies and recreation facilities to benefit from both the investment made and the rigorous security procedures completed and continuously monitored. Facilities listed on Recreation.gov can enjoy security while focusing on what they do best – managing the country's federal lands and waters. To find out more about the Recreation.gov platform or lessons learned during the ATO process, contact us.

CONTACT US

WILL HEALY:
Healy_Will@bah.com

JJ GORSUCH:
Gorsuch_JJ@bah.com

AT A GLANCE:
ATO TECHNICAL REQUIREMENTS

A system must meet hundreds of technical requirements, or controls, before it may receive an ATO. The controls are grouped into 17 "Control Families." The controls are split into three categories based on impact: low, moderate, and high. Reservation systems that handle names and contact information are considered Moderate or High. The table below provides the number of controls per family by category.

FISMA COUNT OF BASELINE CONTROLS BY CONTROL FAMILY

CONTROL FAMILY	LOW	MODERATE	HIGH
AC: Access Controls	11	17	18
AU: Audit and Accountability	10	11	12
AT: Awareness and Training	4	4	4
CA: Security Assessment and Authorization	7	7	8
CM: Configuration Management	8	11	11
CP: Contingency Planning	6	9	9
IA: Identification & Authentications	7	8	8
IR: Incident Response	7	8	8
MA: Maintenance	4	6	6
MP: Media Protection	4	7	7
PS: Personnel Security	8	8	8
PE: Physical and Environmental Protection	10	16	17
PL: Planning	3	4	4
RA: Risk Assessment	4	4	4
SC: System and Communications Protection	10	19	21
SI: System and Information Integrity	6	11	12
SA: System and Services Acquisition	6	9	13
TOTAL	**115**	**159**	**170**

Source: NIST Special Publication 800-53 (Rev. 4)

These security controls are comprehensive and some of them impact systems at a foundational level. If the security requirements were not considered when the system was designed and built, it is most likely not compliant. Foundational requirements are difficult to address in hindsight because addressing them will likely have a ripple effect, increasing time and expense. The following table describes a sample of changes that will likely have an impact.

CONTROL	DESCRIPTION	IMPACT
Access Control and Authentication	All components of the system need to meet session and authentication requirements. For example: • Minimum password length and complexity • Old passwords cannot be reused • Inactive accounts need to be disabled after 90 days of inactivity • Privileged accounts authenticate with MFA	Most custom and COTS applications do not meet all of the required controls. **Custom authentication and authorization functionality will need to be rewritten. COTS products will need to be replaced,** unless they can leverage a specialized Single Sign On (SSO) system to meet these requirements. In that case, the **new SSO must be purchased, hardened, and integrated** with any component that a user or administrator can log in to. Identity and Access management components should be **installed by SMEs** as they are unique, and the impact of misconfiguration is high. The new SSO component must also meet all of the FISMA requirements. **User information will have to be migrated** from all of the application components to the SSO system. **Each of the components will have to be rewritten** to accept user identities and properties from the SSO instead of the legacy authentication mechanism.
Boundary Protection	The information system needs to implement controls that separate it from other networks, including the internet. Communications that pass the system boundary must be monitored and controlled.	A firewall and intrusion prevention system (IPS) must be procured. They are **expensive and multiple systems will be needed** for redundancy. The firewalls must be configured and tested to support each endpoint. Once deployed, it will almost certainly generate false positive blocks that **disrupt users and require immediate attention.**
Secure Coding	A secure coding standard must be developed and implemented as part of the software development lifecycle.	A secure coding standard must be developed and the entire code base must be reviewed against the standard. The coding standard must account for common vulnerabilities, such as OWASP Top 10, as well as emerging vulnerabilities and technology specific vulnerabilities. If the original code base wasn't written with a secure coding guideline in mind, **the front end, input methods, logging, data access layer, and user management functionalities would likely need to rewritten.**

CONTROL	DESCRIPTION	IMPACT
Encryption in Transit	Network connections must be encrypted in transit with FIPS 140-2 validated modules.	Unencrypted network connections must be encrypted. This will require application changes. Encryption must be executed with FIPS 140-2 validated modules, which are normally only found on systems designed to meet Federal government standards. If the system's encryption modules have not be validated, **the system will likely need to replaced.**
Encryption at Rest	System data is encrypted at rest, including files, cache, databases, queues, and disks.	Existing databases that are not designed with encryption would **require a complete rewrite** to accommodate different field types and sizes. **All database queries would need to be rewritten** to allow for encryption and decryption when creating, modifying, or reading any information from the database.
Auditing	Logs must be collected from all systems and analyzed.	Accredited systems require a Security Incident and Event Monitoring (SIEM) system to collect and analyze logs. One will need to be purchased, installed and configured. **All systems must be reconfigured** to send logs to the new SIEM. **The security team will need to create threat models for the system that describe potential targets and attack vectors. Security alerts must be built to monitor these attack vectors and tested periodically.**

Depending on the system architecture and size, it can be more cost effective to rebuild parts or all of the system rather than reviewing and remediating all deficiencies. Smaller systems will likely not include all of the security capabilities, like Single Sign On systems, SIEMs, Firewalls, IDS, Antivirus, Integrity Monitoring, Configuration Management tooling, etc. If the system is not hosted in an accredited data center, it would need to be migrated.

Large or enterprise systems have greater economies of scale and likely more common security tooling. In these scenarios the larger systems will require longer audits and have more findings due to the size. Remediations are also likely to take longer because they tend to be larger in scope. Also, the system must be isolated from the rest of the data center or enterprise at the network level. If it's not, the network must be modified so that the system sits in a dedicated subnet with boundary protections aligned with the applicable controls.

CONTACT US

WILL HEALY:
Healy_Will@bah.com

JJ GORSUCH:
Gorsuch_JJ@bah.com