Ensuring that these privileges are removed when a contractor no longer requires them is key to maintaining a secure organization.

SailPoint Access Certification

The Challenge

Account attestation and certification present several challenges for government agencies. Employees and contractors need access to the right technology and facilities at the right time, but accounts also need to be terminated in a timely manner. On top of that, users need to maintain the least privilege to resources to perform their duties to reduce the organization's security risk. Attesting and certifying access is a complex issue for every agency.

FAR clauses require contracting officers and contracting officer representatives to govern and attest to the access contractors are receiving as part of their projects. Regular validation is necessary since contractors frequently roll on and off contracts or are granted access on a temporary basis. Ensuring that these privileges are removed when a contractor no longer requires them is key to maintaining a secure organization.

Maintaining accurate access records can be particularly challenging in government agencies, which often have the critical data spread across many different systems—or the information may be out-of-date or stale. Other problems include governing contractors on multiple contracts, dealing with timely contract extensions, and employees moving between jobs.

As agencies move to the cloud and towards Zero Trust security initiatives, identity management grows more important. Gartner's How Risk Is Managed Across Infrastructure report predicts that by 2021, organizations with complementary/integrated identity governance capabilities across applications and files will suffer 60% fewer data breaches.

The Solution

When government agencies want to address such challenges, most vendors will approach them with a blank piece of paper. They write down the details of the problem, go away, and come back in a couple of weeks or months with a solution that they can custom build for the agency. The drawings go back and forth for months through multiple approval boards; fully deployed solutions can take years.

SailPoint and UberEther have already built that solution.

Using SailPoint as a platform, UberEther has built Integrated Identity, Credential, and Access Management (ICAM) specifically for government customers. If your agency is struggling with an issue relating to identity management, we have everything to be successful already built—before we even walk through your agency's door.

"Managing the lifecycle of employees and contractors in the government takes very specific domain knowledge. Having worked with numerous government agencies over the last 10 years, UberEther already developed the government-specific best practices and workflows to accelerate each agency's identity governance solution. We understand the complications of government hiring and managing contractors to the FAR. Let us help you make identity governance a business enabler and not just a compliance checkbox," says Matt Topper, President and Solutions Catalyst at UberEther. Our solution already has more than 40 use cases for managing employees and contractors.

Each use case is defined through simple, easy-to-follow diagrams outlining these best practice solutions which have already been coded, tested, and validated in multiple government agency production environments. Not only do we focus on the happy path solution, we also build in the processes to enhance data quality at each step, something that all government agencies struggle with. We have already thought through the problems and developed solutions. You don't need to reinvent the wheel.

RESOURCES

Identity Governance Addresses US Government Cybersecurity Frameworks
carah.io/Sailpoint-IG-Blog

How Identity and Cloud Governance Enhances NSA Guidance for Improving Cloud Security
carah.io/Sailpoint-IG-NSA-Blog

Identity for Government Page
carah.io/Sailpoint-Identity-Governance

SailPoint | carahsoft | uberether

While other vendors might spend 6 to 12 months working through review and approval boards just to get the diagrams written, we can walk in with code that has been running in production for government agencies for over five consecutive years.

Results

UberEther addresses the government's unique access certification issues. When a 90-day certification is due, the system gives the contracting officer a list of contractors so they can quickly approve who remains on the contract. The system automatically offboards anyone who is no longer on the contract. If it is that contractor's only contract or their last contract, the system completely offboards them from the agency and disables their external access.

The solution is even designed to handle situations with incomplete or out-of-date information. It uses certifications to sort through the records and create reports of your agency's contracts, contracting officer representatives, and people who no longer work for the agency. It can identify contracts with CORs that do not fit or provide a list of employees with managers who are no longer employed by the agency.

Our solution is even capable of handling situations like an employee or contractor switching positions within the government. We establish access to both the new and old jobs during a time of transition when the employee will be wearing two hats. The old manager can certify access as needed, specifying access to one system for 14 days and another for 30 days. After the transition, all the access for their old position is automatically removed.

Our experience with government can make your life easier in many other ways. We have created a fully end-to-end automated process to complete Form 2875 digitally. We are familiar with governing contractor access through FAR regulations and everything necessary to comply with the FICAM Architecture and Roadmap, OMB M11-11, and OMB M19-17. We can comply with NIST SP 800-53 Access Controls from day one.

In addition, UberEther greatly reduces your implementation costs. While other vendors might spend 6 to 12 months working through review and approval boards just to get the diagrams written, we can walk in with code that has been running in production for government agencies for over five years. All the bugs have already been ironed out, and the best practices are in place. Our solution is up and running in production before other vendors have agreed on the diagrams and started coding.

Key Benefits

- Streamline access reviews and certifications
- Grant and revoke access based on attribute-backed policies without manual mitigation
- Enable security policies automatically and provide faster service
- Provide policy-based access control using standardized security hierarchies that have been proven for more than a decade

CONTACT US **Maggie.Manfredi@carahsoft.com • (703)-230-7488 • www.carahsoft.com/vendors/sailpoint

© 2020 Carahsoft Technology Corp.