USDA: IDENTITY AND ACCESS MANAGEMENT TOOL AUTOMATES PROCESSES AND SAVES RESOURCES DEPARTMENT-WIDE

The Cybersecurity and Infrastructure Security Agency's Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their respective security postures by delivering better visibility and awareness of their networks and defending against cyber adversaries.

In 2019, the U.S. Department of Agriculture (USDA) began replacing its legacy Identity and Access Management (IDAM) platform with a new IDAM tool through CDM—a process that increased the efficacy of user lifecycle automation processes, reduced administrative costs, and strengthened overall cybersecurity. This effort also set the stage for USDA to adopt a centralized approach to support the IDAM needs of the department's 29 agencies and offices.

CDM ASSISTANCE

USDA's legacy IDAM solution was well-established but no longer keeping up with the department's evolving needs or changing industry standards. The legacy tool's aging software also made it vulnerable to cyberattacks, and it was not fully scalable to meet USDA's goal of centralized IDAM management.

The CDM Program offered a modern, industry-leading IDAM tool that could begin to address USDA's needs. The initial project incrementally introduced the new tool's capabilities into the department's processes to demonstrate the value for future broad implementation throughout USDA. This involved building automated workflow processes for USDA's Integrated Lifecycle Management (ILM) capability, such as hiring new employees and processing the departure or transfer of personnel. Before introducing the new ILM capability, these actions triggered a series of information technology (IT) actions, including assigning email addresses, modifying user access to domains, and issuing or rescinding personal identity verification credentials.

> *"We knew that alleviating the bottleneck would help everything move faster, better, and less problematically. The results were better and more far-reaching than we ever anticipated."*
>
> **Adam Zeimet**
> ICAM Branch Chief,
> USDA

The legacy USDA IDAM system's reliance on manual inputs for these tasks was prone to errors. Correcting problems was time-consuming and costly. Additionally, security vulnerabilities could arise when departed employees continued to hold their credentials to access systems. Even a simple personnel shift of moving divisions could create "privilege creep" where employees maintained access to their previous groups.

The new ILM capability provided a way for USDA to reduce or eliminate paperwork and human error. Additionally, the new solution aligned with guidance from the Federal Identity, Credential, and Access Management (FICAM) Architecture and playbooks, bringing USDA into alignment with identity policy requirements. Using the CDM Request for Services process, USDA set up and began using ILM within a few months. "We went through an agile and incremental development process that allowed us to be flexible with use cases and requirements as we implemented the new tool," said USDA's Identity, Credential, and Access Management (ICAM) Branch Chief Adam Zeimet. "We needed to centrally manage a complex business system with a variety of idiosyncrasies and needs and were able to address that and gain a

mechanism that's flexible in implementation, scope, and prioritization of capability."

The USDA team was pleased with the project's progress and the results that quickly and clearly demonstrated the new capability and its value to stakeholders. "It was a lightweight but rapid implementation," Zeimet said. "We've been able to continuously iterate since then to create more value and mature it further."

The ILM implementation was well-timed, coinciding with the new and evolving Office of Management and Budget (OMB) and federal ICAM requirements. "We got ahead of the curve on this, which, along with cross-agency priority goals, gave us a tailwind that allowed us to meet and exceed those goals," Zeimet said. "We worked with a variety of stakeholders, identifying unique challenges and needs along the way, and through it all we were able to nimbly respond, deliver value quickly, and demonstrate success as we went through the process and maintained support."

IMMEDIATE IMPACT

USDA spent more than two years building and implementing its legacy IDAM system; in contrast, the new CDM ILM capability introduced in February 2021 was operational and benefitting the department within a few months. "Since then, we have been adding new capabilities and features, improving and iterating in real time," Zeimet said.

From a security perspective, USDA now has a complete top-down view of all identities and access across the entire department, which is something it lacked before. Reducing human error from the user lifecycle management process also dramatically decreased security vulnerabilities. User identity and permissions-related actions now occur almost immediately rather than being placed in a backlog, significantly lessening the number of separated or transferred personnel accounts with improper access after the personnel action occurred.

Operationally, USDA has saved numerous hours and staff-related costs through increased automation. The department now requires only minutes to handle onboarding, transferring, and offboarding actions—a dramatic improvement compared to the days and weeks of work time required in the past.

The USDA Forest Service provided an excellent use case for the new ILM capability. Each year, the Forest Service hires more than 6,000 seasonal firefighters and emergency responders. The rapid personnel onboarding process in the spring and the offloading process at the end of summer stressed USDA's systems, took six weeks or longer to complete, and led to backlogs of ongoing IDAM requests. Using ILM to automate this hiring process eliminated a huge strain on Forest Service personnel. Past needs had necessitated expanding the internal administrative team by as much as 300 percent to manage the workload; the new capability *saved* the agency approximately 1,900 hours of staff time in one season and eliminated the annual backlog. Furthermore, if employees return next season—as many do—USDA can easily return them to active status "with a quick flip of the switch," according to Zeimet.

USDA quickly realized similar savings for user lifecycle management actions across the department. "Reducing the manual work is not just cost-effective but also is more secure, reliable, and faster and leads to better customer experiences," Zeimet said. In addition, with its improved cybersecurity posture, USDA has better positioned itself to advance the federal Zero Trust Architecture initiative.

USDA is also consolidating its end-user IT support, replacing a variety of individual agency offices with a single group that provides IT support services across the department. Applying the automated ILM workflow processes helped USDA manage this large-scale endeavor. USDA adapted and leveraged ILM workflow templates for its agencies while avoiding additional process development and implementation costs and extending improved user experience and cybersecurity advantages throughout the department. "We knew alleviating the bottleneck would help everything move faster, better, and less problematically," Zeimet said. "The results were better and more far-reaching than we anticipated."

THE BENEFIT OF WORKING WITH CDM

Implementing ILM through CDM helped support USDA's goal of centralizing the client IDAM services across the department into its Client Experience Center. Additionally, the funding from CISA to procure the new IDAM tool eliminated a resource barrier in modernizing legacy systems and paved the way for follow-on capability efforts that USDA has been able to self-fund. The CDM Program enabled USDA to rapidly access contract personnel who were already familiar with USDA's CDM solution and overall IT architecture. The CDM system integrator, which collaborated with USDA to define and refine the scope of its requirements, brought the technical expertise needed to implement the project efficiently and more quickly than a traditional contracting process could have.

"Leveraging CDM's expertise and resources was a quick and easy process that enabled us to broaden the [ILM] project throughout the agency and ultimately replace our legacy IDAM platform with a new tool throughout the department," Zeimet said.