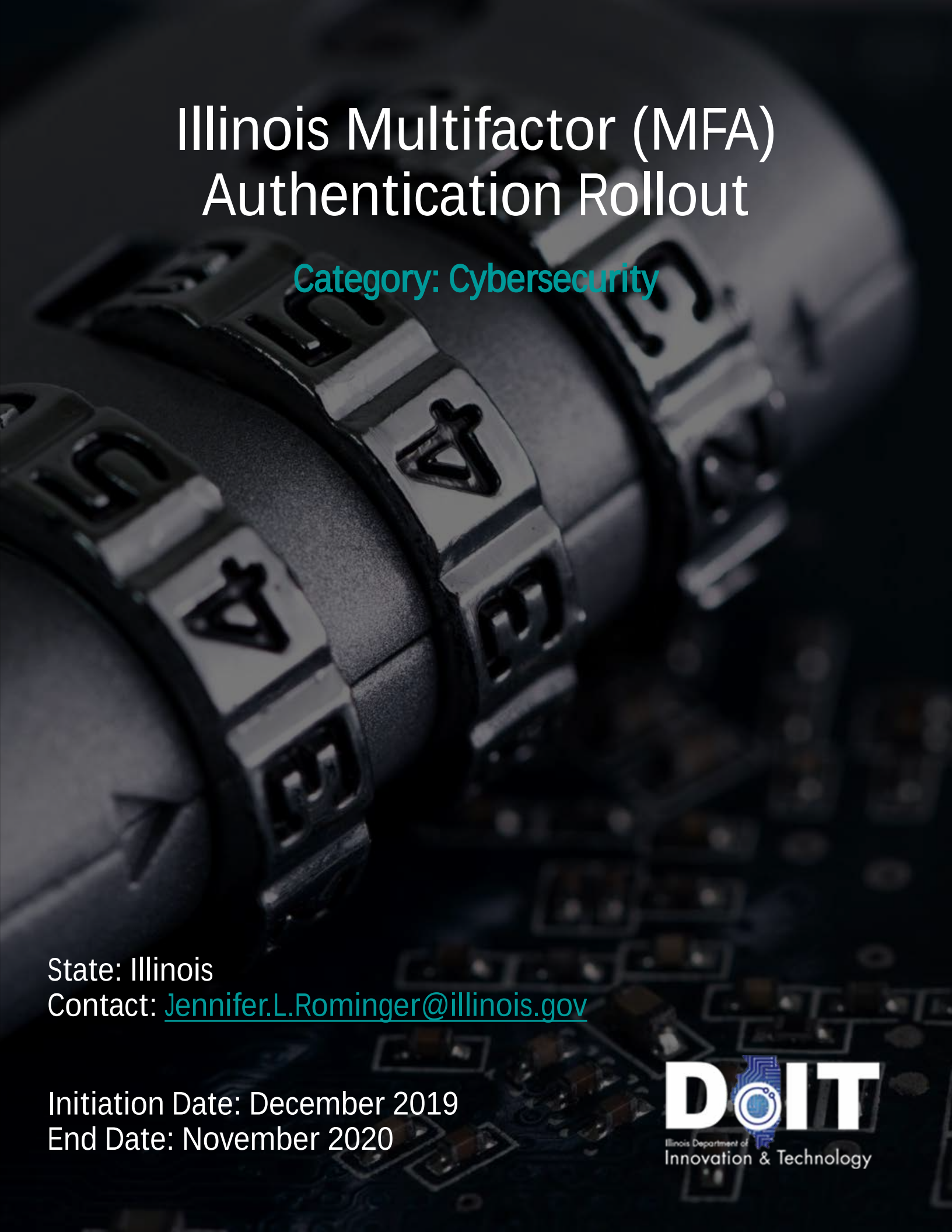
Illinois Multifactor (MFA) Authentication Rollout

Category: Cybersecurity



State: Illinois
Contact: Jennifer.L.Rominger@illinois.gov

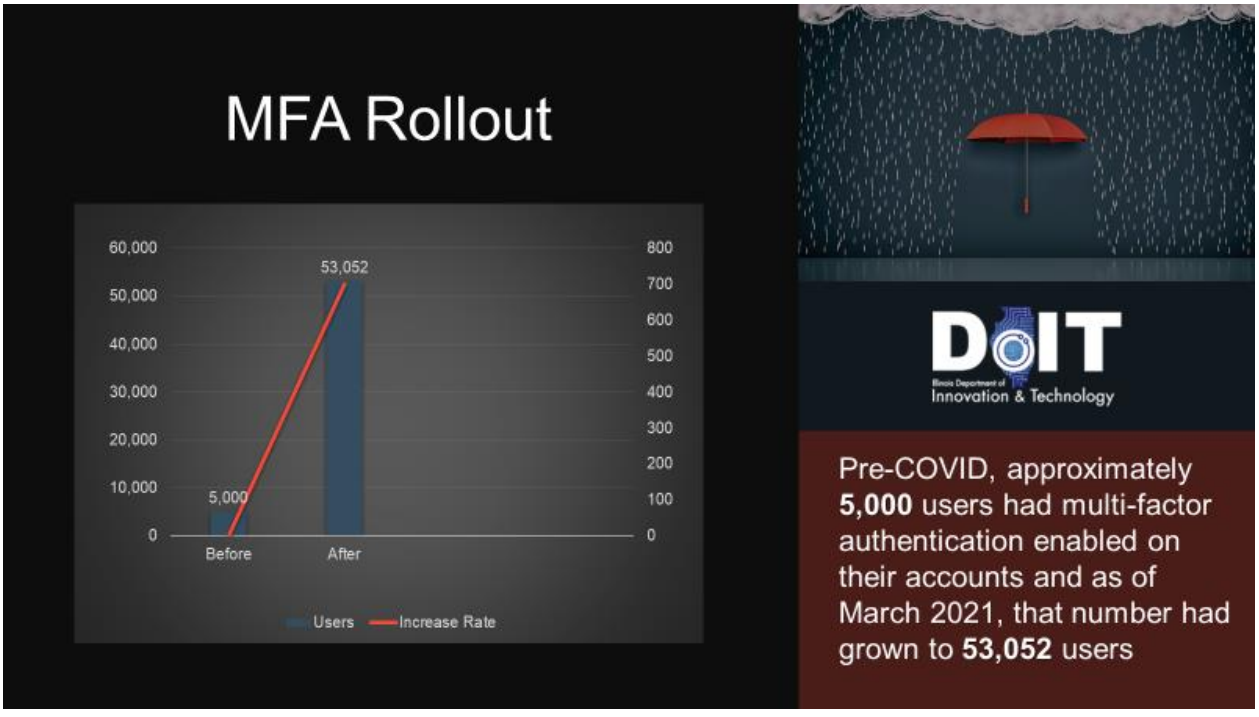
Initiation Date: December 2019
End Date: November 2020

DoIT
Illinois Department of Innovation & Technology

EXECUTIVE SUMMARY

Attacks on government networks have been escalating at an alarming rate over the last few years. To help prevent bad actors from accessing and traversing state networks, DoIT began planning the implementation of multifactor authentication (MFA) for approximately 53,000 accounts. These accounts span approximately 65 different agencies, boards, and commissions serving under the Executive Branch. Illinois Governor Pritzker set the tone and volunteered himself and his staff to pilot MFA for the enterprise.

Mid execution of the project, COVID hit and employees were sent home to work remotely. The team paused rollout and pivoted to support remote work VPN access. Within 8 weeks, the team was able to resume full rollout with only a few changes to the project plan. By early October, all agencies who were using Office 365, had been given ample opportunity to complete their authentication before having their access denied. Due to the upcoming 2020 Presidential elections, a hard deadline was given to set up MFA for remote access on lingering managed accounts. By late November of 2020, MFA became an operationalized process versus a project. MFA account set up is now part of the onboarding process for all new employees.



IDEA

The Department of Innovation & Technology (DoIT) was concerned with having a potential attack on 55,000 user accounts that were only protected by a username and password. In addition, employees had little defense against phishing scams. DoIT decided to move quickly to add an extra layer of security to accounts by implementing MFA.

The MFA roll out project not only helped close a security gap, but it also solved a business problem for many agencies by remediating an audit finding. Government systems and accounts are an attractive target for attack. Threats are increasing every day in number and sophistication. No longer does it suffice to have merely a username and password for login. Ransomware alone has increased over 400% over the last two years. There are many ways to layer defenses, but Multifactor Authentication (MFA) is a security process that makes it harder to data or information. MFA blends at least two separate factors required for account login. Factors typically include a combination of:

- Something you know – such as username and password
- Something you have – such as a cellphone
- Something you are – such as fingerprints or other biometric data

“Information security” means making sure data is kept confidential, has integrity and is available. Professionals working in the security arena help inform the business of risk and assist management in making risk-based decisions regarding the systems they operate. In Illinois state government, DoIT is the IT service provider for state agencies, boards, and commissions serving under the Executive Branch. State government not only provides essential services to the public, but is entrusted with sensitive information. Protecting those services and sensitive data has to be aligned with risk. Enabling MFA on employee accounts changes the way in which they access data and systems when not on a state network. While having the flexibility of a mobile workforce increases productivity, it also increases risk. When the project to roll out MFA was originally planned, the business rationale did not include a pandemic. No one could have anticipated that within three months of kicking off the MFA project, the entire state workforce would become remote.

While evaluating potential costs, it was determined that the procurement cost was low as the state already had some tools available, as well as the in-house talent to configure MFA. The time to set up each employee was also extremely low. The true cost was in staff hours to develop the concept, run a pilot, change procedures, write training, support help desk calls, communicate to agencies what to expect and stand up an MFA deployment team. While the risk of not implementing MFA was high, the estimated cost to implement MFA was relatively low. The decision to kick off the project was easy.

Perhaps the most unique feature of this MFA rollout was the pilot group selected. As expected, the security division first tested the process in Beta. The security training section captured the user experience and worked with technical staff to craft the directions and create processes and procedures. The true pilot group was comprised of the highest level executive staff in state government. The Governor volunteered his staff to go first and pilot the process and provide feedback on issues and concerns. We typically roll out to the Governor's Office after the process has been refined and tested. A significant reason for choosing this pilot group was to demonstrate the importance of promoting the project.

The adoption of MFA is an important consideration in the public sector. Microsoft estimates that accounts using MFA are 99.9% less likely to be compromised[i]. Also, per Homeland Security Presidential Directive 12, federal agencies are required to use enhanced user authentication, data security and information assurance. The adoption of MFA is one the top three things the security experts can do to protect their environment and is considered fairly easy to implement. In early 2020, it was estimated by the LastPast company that only 57% of organizations have globally deployed MFA.

IMPLEMENTATION

The roadmap for the MFA project began when it was named a top security initiative for DoIT. Because DoIT had previously and successfully rolled out Office 365 to the same population of users, they chose the same model for the MFA rollout. This project was managed in a traditional waterfall project management approach. The project utilized the typical processes of initiating, planning, executing, monitoring and controlling, and closing. After developing the work plan and getting approval from stakeholders, a tiered rollout plan was agreed upon. At the end of the rollout, MFA was operationalized for all DoIT teams as new employees were onboarded and offboarded.

The Illinois MFA project began with a strong project sponsor and documented stakeholders. The Governor's Office advocated for the project and was informed of the project status throughout the rollout. There was not one group of employees across the enterprise who remained exempt from the project or without a role. Agency Directors and CIOs were informed of their "place in line" for rollout and were identified as the second group to pilot the process. Agency Directors and CIOs were strong advocates for ease of setup and importance. Every employee was notified to set up by a certain date and given instructions. After their setup date had passed, MFA was enforced on their account. If the user failed to follow directions after multiple reminders from multiple sources, they were locked out of their account when attempting access.

Communicating with so many employees across agencies was a challenge. An executive level communication from the CISO went to all agency directors and CIOs setting expectations, outlining what was going to occur, and giving them a project lead as a point of contact. At that same level, executive briefings enforced to agency directors that this was mandatory. The next level of communication was directly to the CIOs of each agency with a cadence of communication at the agency level in the weeks prior to rollout. The project team provided a message template for the agency to customize to inform their employees of the MFA rollout. The next tier of communication was from the DoIT.MFADeployment team directly to employees. This communication informed them what needed to be done, why, completion date, who to contact for help, and a full set of directions and FAQs. Reminders were sent weekly three to four weeks before their access was shut off. Reports on progress were given to agency CIOs.

Before getting started, the state was in the process of procuring SaaS solutions to reinvent Identity and Access Management. Procurement in the government arena is a slow process. The dilemma was deciding to wait until the procurement was completed before implementing MFA or use some of the tools available to begin securing accounts immediately, knowing that in the next couple of years, another version and layer of MFA would be coming. The decision was made to add security now versus the risk of waiting. The actual cost of buying a solution was zero.

The next decision point was in deciding where MFA would reside in the architecture. DoIT engineering teams established the rules and groups needed to test a proof of concept. Enabling MFA on accounts created problems with how state mobile phones synced with email. This challenge broadened the scope to include a download and setup of a new email application on approximately 8,000 state iPhones and iPads.

IMPACT

The reason for and benefit of implementing MFA across the enterprise was enhanced security. The business rationale was to reduce risk in delivering service across the state. The goals were accomplished. The implementation of MFA represents a shift from outdated authentication methods towards modern identity and access management in Illinois government.

MFA was initiated, planned, and launched pre-pandemic. The rollout had just hit its stride when work from home was first being discussed. The benefits and impact of the project grew exponentially as risk grew. While the MFA deployment team had to pause and readjust the rollout cadence and messaging, the pandemic delayed the project only 8 weeks. Towards the end of the project, the timeframe was condensed to defend against potential security risks presented by the upcoming Presidential Election of 2020. It was decided that all MFA would be enabled prior to the election.

The current version of MFA is part of the onboarding process and help desk ticket routing. The long-range plan is to expand the scope of MFA for employees, as well as citizens accessing services. Employees with privileged access will have to authenticate frequently. Single sign on for external facing applications accessed by the public will be transformed and SaaS solutions employed. The day will soon come when a username and password will no longer suffice to prove identity within government systems.

Modernizing identity and access management is essential to serving citizens securely. The cost of this project was low, while the payoff is high. The stage has been set for a new culture of security in Illinois state government. Pre-covid, Multi-factor Authentication (MFA) had been enabled on approximately 5,000 user accounts. As of March 2021, MFA had been enabled on approximately 53,052 accounts. Security is becoming a part of the business model. If services are important, and we are to retain the trust of our agency users and citizens of Illinois, security matters. Systems and assets should be secured commensurate with risk. MFA is a low-cost, high return on investment project.

[i] Your Pa$$word doesn't matter - Microsoft Tech Community