IDENTIV WHITE PAPER

Mandating Multi-Factor Authentication for Cybersecurity in the U.S. Federal Government

Identiv's Proactive, Passwordless Approach to Protecting Critical Network Infrastructure and Data

Introduction

The United States federal government relies heavily on information technology (IT) to drive efficiencies and increase public engagement. However, an increase in cyberattacks and data breaches impacting government operations creates a storm of risks and challenges.

Cybersecurity risks massively impact department and agency operations, eroding public trust and decreasing the capability to deliver mission-critical functions.

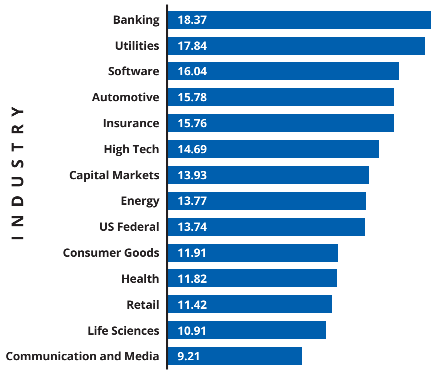
In response to damaging cyberattacks, data breaches, budget pressures, and public expectations, the U.S. government is changing how it addresses cybersecurity risks. Currently, it uses four key strategies to protect its sensitive data and safeguard its critical infrastructure:

- **Proactive cyber threat hunting[1]**
- **Increased use and sharing of cyber intelligence data[2]**
- **Continuous security monitoring, with a focus on boundary protection and security event lifecycle management[3]**
- **Automation and orchestration of security operations[4]**

Since 2017, the U.S. government continues to increase investments to execute these strategies, focusing on defending against and mitigating cyberattacks. It is expected these investments will continue to grow in 2021 and beyond as agencies tackle increasingly advanced and persistent cybercriminals.[5]

Current Situation of Cybersecurity in the U.S. Government

In 2018, the U.S. was the country most severely affected by cybercrime in terms of financial loss. Industry experts estimate that the U.S. government faced costs of over 13.7 billion U.S. dollars as a result of cyberattacks.



Average annual costs caused by global cybercrime in 2018, by industry sector (in million U.S. dollars)[6]

In March 2021, hackers acting on behalf of a Russian intelligence agency breached email systems at the Treasury and Commerce Departments.

According to federal and private experts, the cyber attackers broke into a range of important government networks, including in the Treasury and Commerce Departments, and gained free access to their email systems.[7]

The reason for the attack on the agency and the Treasury Department remains abstract, but according to several corporate officials, the attacks progressed since Spring 2020, meaning they continued unnoticed through months of the pandemic and the election season. This incident is regarded as one of the most sophisticated and perhaps largest hacks in more than five years.

In early April 2021, at least two groups of China-linked hackers spent months using a previously undisclosed vulnerability in American virtual private networking (VPN) devices to spy on the U.S. defense industry.

[1] U.S. Department of the Interior Office of Inspector General (2017). Threat Hunting: A Proactive Technique for Finding Sophisticated Cyber Threats.

[2] Richard Bejtlich, OP-ED (2015). Will Sharing Cyberthreat Information Help Protect the United States?

[3] U.S. Federal Government. Department of Homeland Security (2018). Continuous Diagnostics and Mitigation (CDM).

[4] FCW: The Business of Federal Technology (2018). Why DHS is changing the way agencies connect to the internet.

[5] Whitehouse.gov (2018). CyberSecurity Funding.

[6] https://www.statista.com/statistics/474928/average-annual-costs-caused-by-cyber-crime-worldwide/

[7] NY Times (2020). Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect.

According to Charles Carmakal, Senior Vice President at Mandiant, "Hackers were operating from US digital infrastructure and borrowing the naming conventions of their victims to camouflage their activity so they would look like any other employee logging in from home. We are seeing pretty advanced tradecraft."[8]

A recent ransomware attack against Colonial Pipeline significantly impacted the flow of refined oil across America. The federal government issued an emergency declaration for 17 states and the District of Columbia after the country's largest fuel pipeline went down. Gasoline price hikes and shortages were reported across the country. Colonial paid almost $5 million as a ransom to unlock its systems.[9]

Some other recent significant cyber incidents include:[10]

March 2021

The U.S. Cyber Command conducted more than 12 operations to confront foreign threats ahead of the 2020 U.S. elections, including 11 forward hunt operations in nine different countries.

U.S. Cyber Command confirmed it assisted Columbia in responding to election interference and influence operations.

Chinese government hackers targeted Microsoft's enterprise email software to steal data from over 30,000 organizations around the world, including government agencies, legislative bodies, law firms, defense contractors, infectious disease researchers, and policy think tanks.

February 2021

The U.S. Department of Justice accused three North Korean hackers of conspiring to steal and extort over $1.3 billion in cash and cryptocurrencies.

North Korean hackers attempted to break into the computer systems of pharmaceutical company Pfizer to gain information about vaccines and treatments for COVID-19.

February 2021

Unknown hackers attempted to raise levels of sodium hydroxide in the water supply of Oldsmar, Florida by a factor of 100 by exploiting a remote access system.

December 2020

Over 200 organizations around the world, including multiple U.S. government agencies, revealed breaches by Russian hackers who compromised the software provider SolarWinds and exploited their access to monitor internal operations and exfiltrate data.

Iranian state hackers used a Christmas theme for a spear-phishing campaign targeting think tanks, research organizations, academics, journalists, and activists in the U.S., Persian Gulf, and EU.

CISA and the FBI announced that the U.S. think tanks focusing on national security and international affairs were targeted by state-sponsored hacking groups.

November 2020

U.S. Cyber Command and the NSA conducted offensive cyber operations against Iran to prevent interference in the forthcoming U.S. elections.

October 2020

The U.S. government announced Iranian hackers targeted state election websites to download voter registration information and conduct a voter intimidation campaign.

The FBI and CISA announced a Russian hacking group breached U.S. state and local government networks, as well as aviation networks, and exfiltrated data.

CISA: Securing Federal Networks

On November 16, 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018.[11] This breakthrough legislation elevates the mission of the former National Protection and Programs Directorate (NPPD) within DHS and establishes the Cybersecurity and Infrastructure Security Agency (CISA).

CISA builds the national capacity to defend against cyber-attacks and works with the federal government to offer cybersecurity tools, incident response services, and assessment capabilities to safeguard the ".gov" networks supporting the essential operations of partner departments and agencies.

The federal enterprise depends on IT systems and computer networks for vital operations. These systems face large and diverse cybersecurity risks that range from unsophisticated hackers to technically skilled intruders using advanced intrusion techniques. Many malicious attacks are designed

[8] Reuters (2021). China-linked hackers used VPN flaw to target U.S. defense industry researchers.

[9] CNBC (2021). Colonial Pipeline cyberattack is no cause for panic – here's why.

[10] CSIS.org (2021). https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[11] https://www.dhs.gov/topic/cybersecurity

to steal information and disrupt, deny access to, degrade, or destroy critical IT systems.

CISA works with each federal civilian department and agency to promote the implementation of common policies and best practices that are risk-based and able to effectively respond to the speed of ever-changing threats.

As systems are protected, alerts can be issued at machine speed when events are detected to help protect networks across the government IT enterprise and the private sector.

This enterprise approach transforms the way federal civilian agencies manage cyber networks through strategically sourced tools and services that improve the speed and cost-effectiveness of federal cybersecurity procurements and allow consistent application of best practices.[12]

Executive Order on Improving U.S. Cybersecurity

The recent cyberattacks exposed areas of weakness in critical U.S. infrastructure assets. This is why President Biden signed a new Executive Order (EO) to help strengthen the country's cybersecurity.[13]

A key part of the EO necessitates agencies to adopt multi-factor authentication (MFA) and encryption for data at rest and in transit to the maximum extent possible.

Federal Civilian Branch Agencies will have 180 days to abide by the EO and need to report on progress every 60 days until the adoption is complete.

If for some reason agencies cannot fully adopt MFA and encryption within 180 days, they must report to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA with a justification for not meeting the deadline.

The EO is an important step forward as it clearly prioritizes protecting every account with MFA without mandating any specific technology. It no longer limits MFA to the PIV/PKI platform that agencies have relied on for more than a decade.

This is an outstanding move, as even the weakest forms of MFA can stop some attacks where passwords are the attack vector.

FIDO Authentication is the only standards-based substitute to Personal Identity Verification (PIV) for applications requiring protection against phishing attacks. This EO opens the door for agencies to deploy FIDO Authentication, which they perhaps wanted to do but were held back as the use of any non-PIV authentication was not permitted earlier.[14]

Fast IDentity Online (FIDO) Authentication for Cybersecurity

Based on free, open standards from the FIDO Alliance, FIDO Authentication enables password-only logins to be replaced with secure, fast login experiences across websites and apps.

FIDO works by using standard public-key cryptography to provide strong authentication and leave zero data at rest. FIDO U2F is an open standard that provides additional security and streamlines Universal 2-Factor authentication.

FIDO2 is the term for FIDO Alliance's latest set of specifications. FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments.

The FIDO2 specifications are the World Wide Web Consortium's (W3C) Web Authentication (WebAuthn) specification and FIDO Alliance's corresponding Client-to-Authenticator Protocol (CTAP).

The FIDO Alliance's FIDO2 protocols for passwordless authentication allow government institutions to harness mobile technology for easier authentication in multiple channels.

Since FIDO2 credentials are cryptographically registered to a user's enrolled device, they cannot be easily shared by users, unlike passwords.

Leveraging cryptographic login credentials coupled with biometric strong authentication, fraudulent individuals can be prevented from accessing government data.

uTrust FIDO2 GOV Security Keys

For government and regulated agencies, Identiv's uTrust FIDO2 GOV Security Keys (available late 2021) meet FIPS 140-2 and NIST guidelines for high-assurance strong authentication.

uTrust FIDO2 GOV Security Keys are the perfect strong near field communication (NFC) authentication device, providing FIPS 140-2 validation and assurance level 3 (AAL3) of NIST SP800-63B guidance for regulatory compliance.

[13] Whitehouse.gov (2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[14] FIDO Alliance (2021). FIDO Alliance Supports Biden Administration EO on Cybersecurity.

The keys are ideal for government employees or contractors (desktop and mobile), citizen access to government services, public safety and first responders, and emergency communications personnel.

With multi-protocol FIDO U2F, FIDO2, smart card (PIV), and One Time Password (OTP) support, these security keys are resistant to phishing attacks, safeguarding your credentials and accounts.

- **Type A and Type C GOV Security Keys: Robust, hardened security devices for governments and other regulated industries.**
- **Enterprise Security Keys: Ideal for small-to-enterprise organizations that do not require FIPS 140-2 validation**

Benefits of uTrust FIDO2 GOV Security Keys

Here is how Identiv's uTrust FIDO2 GOV Security Keys can help government agencies:

- **Strong authentication protocols: The keys prevent data from being breached by phishing or brute-force attacks by strengthening authentication protocols.**
- **Passwordless approach: uTrust FIDO2 GOV Security Keys provide a simple, strong authentication experience eliminating the need for passwords.**
- **Multiple options: The security keys support both contact (USB A/C) and contactless (NFC) use-cases, providing multi-protocol FIDO U2F, FIDO2, smart card, and OTP support.**
- **Public-key cryptography: The solution is based on public-key cryptography, which means keys stay on the device. There are no server-side shared secrets to steal.**
- **Advanced protection: It protects against phishing, man-in-the-middle, and replay attacks. There is no linkability between services or accounts and no third party in the protocol.**
- **Lower costs: Security keys have lower development/ maintenance costs and little-to-no provisioning costs. User-friendliness ensures faster time to market and future-proofing. It also ensures lower breach risks, potential damages, and password reset costs.**
- **Compliance: uTrust FIDO2 GOV Security Keys are Trade Agreements Act (TAA)-compliant and assembled in the U.S.**

Conclusion

Changes to the U.S. federal government's security program capabilities in 2021 are key elements of a paradigm shift from a previously federated, decentralized, and reactive cybersecurity basis, to a consolidated, centralized, and proactive approach to protect critical network infrastructure and cybersecurity data.

This signifies a momentous transformation in how departments and agencies at all levels are guaranteeing the security and operational willingness of their IT networks.

Identiv expects that, over time, these changes will result in improved coverage of protective capabilities and a stronger capacity to adapt and meet the government's growing threat landscape.

The U.S. government should consider including hardware security key-based MFA into their security strategy because without two-factor authentication, they are increasing the vulnerability of their network and their organization.

About Identiv

Identiv is a global leader in seamless authentication and security solutions. We verify frictionless access and anywhere operations, protect identities from malicious attacks, secure intellectual property, and drive IoT innovation. We digitally secure the physical world.

Learn more by contacting sales@identiv or +1.888.809.8880.

IDENTIV YOUR WORLD, **VERIFIED.**

Identiv, Inc. (NASDAQ: INVE) is a global leader in digitally securing the physical world. Identiv's platform encompasses RFID and NFC, cybersecurity, and the full spectrum of physical access, video, and audio security. For more information, visit **identiv.com** or email **sales@identiv.com.**

© Identiv, Inc. | All rights reserved. This document is Identiv public information.