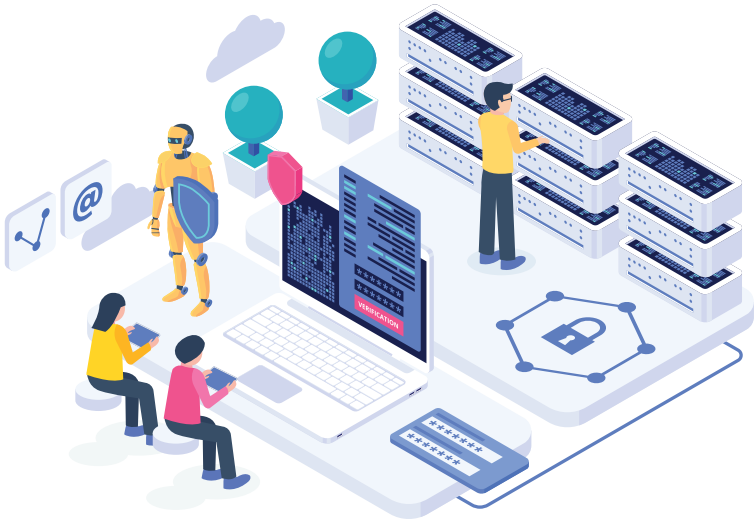
IDENTIV SOLUTIONS BRIEF

Tackling Cybercrime in the U.S. Federal Government with Hardware Security Keys

The U.S. federal government is a complex, heterogeneous ecosystem of departments and agencies creating, disseminating, and storing significant amounts of often sensitive data. The sector is no stranger to the scourge of cybercrime.



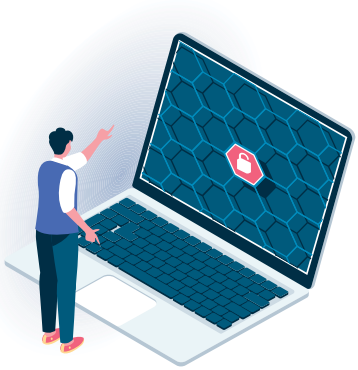
Federal Government, Data Security, and Cybercrime

In 2018, over 31,000 cybersecurity incidents were reported by federal agencies. The following year, the U.S. government accounted for 5.6 percent of all data breaches and 2.1 percent of exposed data in the country. October 2020 saw an attack by Iranian hackers on state election websites aimed at downloading voter registration information and conducting a voter intimidation campaign. Just a month later, multiple U.S. government agencies revealed breaches by Russian hackers.

Earlier this year, the ransomware attack against the Colonial Pipeline severely impacted the availability of fuel across the country.

The current administration has publicly reaffirmed its commitment to ensuring the nation, states, regions, and cities are safe places to live and do business online. It has backed up its statements with action. Earlier this year, President Biden signed a new Executive Order (EO) under which all agencies must adopt multi-factor authentication (MFA) and encryption for data at rest and in transit wherever possible. MFA requires users to provide two or more verification factors to access data via applications, online accounts, or VPNs.

A recently issued data breach notification bill, the Cyber Incident Notification Act of 2021, would "require Federal government agencies, Federal contractors, and critical infrastructure operators to notify the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) when a breach is detected so that the U.S. government can mobilize to protect critical industries across the country."



Increased funding has also been directed towards CISA and the General Services Administration's Technology Modernization Fund to deter and thwart cybercrime and better protect critical national infrastructure.

In August, the CEOs of technology powerhouses Amazon, Apple, and Microsoft met with President Biden to discuss how the private sector and government can better work together to detect and prevent future cyberattacks, especially those targeting critical infrastructure services.

One of the pervasive challenges to building impenetrable federal government cyber defenses is human error, often the weakest link in the security chain. Government employees are prime targets for cyberattacks because they have access to sensitive data, such as financial, economic, and military records. Hackers typically target government employees using phishing scams, posing as trusted sources to access login credentials.

Data, Data Everywhere

Another significant cybersecurity hurdle facing the federal government is the ubiquity of its data. Given the fluid and multifaceted environment in which departments and agencies operate, most do not hold a firm grasp of what data they have or where it is located.

In a recent survey, only 28% of federal respondents said they have full knowledge of where their data is stored, and just one-third claimed to be able to fully classify their data.

Further compounding the challenge, cloud storage is now well on its way into the mainstream in this sector. Over a quarter (29%) of respondents to the same survey said they now store over half of their data in the cloud, and 57% indicated that

31–50% of the data stored in an external cloud is sensitive.

Adequate levels of encryption have not accompanied this large-scale cloud migration. Only 15% of respondents stated that more than half of their sensitive data stored in the cloud is encrypted. This is concerning given the Biden EO clearly states the directive on the matter.

The failure may be due partly to the fact encryption and key management can be complex to deploy and manage, and often requires scarce and expensive cybersecurity skills.

The Way Forward

Federal government agencies must become more intentional about aligning their operations to the latest and most robust industry standards and protocols. This could involve:

- **Pairing Common Access Card (CAC) and Personal Identity Verification (PIV) access with smart card readers, where the CAC/PIV card is the authenticator, and the smart card reader is used in the authentication process**
- **Securing their login.gov accounts with a FIDO security key to prevent phishing attacks from hijacking user accounts and compromising credentials**

Understanding Smart Cards, CAC, PIV, and FIDO Security Keys

U.S. Federal Government Smart Card Programs

Smart card technology is currently recognized as the most appropriate technology for identity applications to meet critical security requirements. Around the world, countries use smart cards for secure identity, payment, and healthcare applications.

The U.S. federal government has standardized on smart cards for employee and contractor identification cards. It is also specifying smart cards in new identity programs for citizens, transportation workers, and first responders.

CAC

One of the most advanced smart ID card programs in the U.S. is the Department of Defense (DoD) CAC, a smart card serving as DoD standard identification for active-duty military personnel, selected reserve personnel, civilian employees, and eligible contractor personnel.

CAC is the principal card used for logical access to DoD computer networks and systems and is the main method of enabling physical access as systems are installed for authentication and access at DoD facilities.

PV

A PIV credential is a U.S. federal government-wide credential used to access federally controlled facilities and information systems at the appropriate security level.

PIV credentials feature certificates and key pairs, PIN numbers, biometrics like fingerprints and pictures, and other unique identifiers. When combined into a PIV credential, it provides the capability to implement MFA for networks, applications, and buildings. PIV credentials can be used for:

- **Authentication for all privileged users, including servers, networks, and applications**
- **Network authentication for all users**
- **Application authentication for all users of an application protecting or containing sensitive information**
- **Access to facilities and buildings**

FIDO Government Deployments

Through its login.gov program, the U.S. General Services Administration (GSA) has rolled out a single sign-on approach across different agency applications. Use of FIDO (Fast Identity Online) is one option. FIDO2 is a set of strong authentication standards enabling users to leverage common devices like on-device biometrics and FIDO security keys to authenticate to online services with phishing-resistant cryptographic security. After a thorough review, GSA found FIDO2's phishing resistance made it the most appropriate approach to address its security challenges.

The login.gov platform provides single sign-on for U.S. public and federal employees to interface and transact with federal agencies online. With one account, users can access services like the federal government's job board, USAJOBS, and the Department of Homeland Security's Trusted Traveler Programs, such as Global Entry.

Other federal bodies have made recent legislative and programmatic moves to boost their levels of data security. These include:

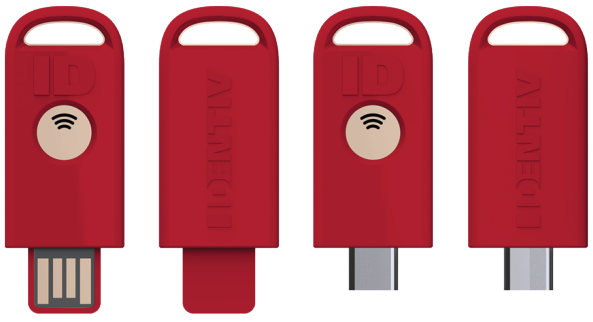
- **National Cybersecurity Center of Excellence: Mobile Single Sign-on for Public Safety/First Responders**
- **NIST: Digital Identity Guidelines: Implementation Resources for SP 800-63-3 Program**
- **Office of Management and Budget: Implementation of OMB memo M-19-17 – FICAM Policy**
- **Drug Enforcement Administration: Electronic Prescribing of Controlled Substances**

While these moves are welcome and warranted, is it feasible to bring a standard, robust approach to what still remains a piecemeal legislative patchwork?
The easiest and most effective option is to invest in hardware-based security keys supporting FIDO2 specifications.

How Can Security Keys Help?

Hardware security keys are increasingly being recognized as the sensible and responsible way to solve the federal government data security challenge.

The beauty of this approach is the authentication process: it is one-touch.



uTrust FIDO2 GOV Security Keys

When users sign into their email or applications, for example, they enter their password and click "sign in". But the process does not end there. They are required to supply a secondary authentication factor to prove they are who they claim to be and are authorized to sign into the account.

At this stage, the user inserts their unique, personal key into their device, presses the button, and access is granted immediately.

In technical terms, what happens here is in the background. A challenge-response exercise is initiated using public-key cryptography between the security key and the service provider. This eliminates the threat of users' accounts being accessed via compromised credentials or a phishing attack.

Closing Thoughts

Federal government agencies need to shift to a mindset where security is implicitly attached to data and the users who need to access it. If they fail to act decisively, they will face a future littered with data breaches that have far-reaching implications.

The good news? Hardware security keys, like those offered by Identiv, put the power (literally) back into their hands and allow them to focus attention on what matters: protecting data and identities.

Identiv's uTrust FIDO2 GOV Security Keys meet FIPS 140-2 and NIST guidelines for high-assurance strong authentication. With multi-protocol FIDO U2F, FIDO2, smart card (PIV), and OTP support, our security keys are resistant to phishing attacks, safeguarding your credentials and accounts.

Visit identiv.com, request a demo, or call +1.888.809.8880 to learn more.