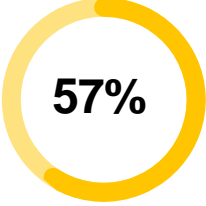# ⊕ A LINEDS

Password Management is Critical for Protecting Government Assets

The largest security gap within government can be closed quickly and cost effectively with strong password policies enforced with an easy-to-use, intuitive, and secure password management solution.

YOUR CYBERSECURITY STARTS HERE!

🔒 @ keeper®

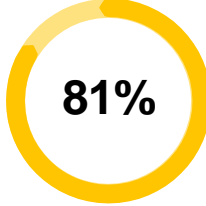**Table of Contents**

ALINEDS

57%

of U.S. Government Agencies
Reported a Data Breach in 2017[1]

21M

records stolen in U.S. Office of
Personnel Management data breach

81%

of data breaches are due to weak,
default or stolen passwords

Government Agencies are Prime Targets for Cyberattacks

Recent cyberattacks at a multitude of Federal Government agencies, and specifically the data breach at the Office of Personnel Management (OPM) in which 21.5 million records were affected[2], underscore the importance of data security and the need for constant vigilance to protect government interests and assets.

Government agencies are targeted in part because they are inadequately prepared to face the challenges ahead. When compared to the cybersecurity performance of 18 major industries, Government ranked 16th, above only Telecommunications and Education[3]. Data held by Government is extremely valuable to cybercriminals. It includes personally identifiable information on government employees, constituents and the public at large, as well as access to classified government assets and intellectual property.

Cyberattacks are growing more frequent and more sophisticated. They are increasingly being led by heavily backed, knowledgeable individuals and state sponsored entities. Cybersecurity Ventures estimates cyberattacks could cost the world over $6 trillion annually by 2021. Government agencies need to implement strong controls to protect their most sensitive assets.

"
Several top secret documents from the NSA and the U.S. Army were discovered on a cloud server without any password protection... Essentially available to anyone with a URL.
"

-2018 Thales Data Threat Report

Poor Password Management is the Root Cause of Most Government Data Breaches

Governments spend immense sums of money on cybersecurity defense and consultants. Beyond the traditional tools like firewalls, system information and event management (SIEM) and anti-virus products, it is easy to get caught up in the most sophisticated threat detection. All of these tools have their place and can be very valuable, however, one problem looms large: **81% of hacking-related breaches leveraged stolen and/or weak passwords.**[4]

Passwords are often the only security measure protecting government agents and assets. Unfortunately, due to human error, negligence and simple lack of knowledge, passwords are also the weakest link in cybersecurity and the most common vehicle for cybercriminals to infiltrate government accounts.

Employees use weak passwords, reuse them across accounts and forget them. These bad password management practices lead to frustration, loss of productivity and puts the organization's security at risk. Forrester found the average employee has 25 work accounts to manage and creating strong, unique passwords for each account is not feasible.

Improving Password Management is a Top Priority for Government Agencies

The U.S. Government has taken initiative to prepare itself for an ever-changing cybersecurity landscape. It has passed several pieces of legislation that specifically mandate agencies to protect their data and provided guidance on how to do so. For example, Executive Order 13800 was passed in May 2017 in response to the recent escalation of cyberattacks on government agencies. The order aims to strengthen the security of federal networks and critical infrastructure, and it places accountability for cybersecurity on each federal agency head.

> **The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises.**[5]

-EO 13800

Executive Order 13800 follows other notable cybersecurity initiatives in recent years. The U.S. Federal Civilian Government Cybersecurity Strategy and Implementation Plan (CSIP), passed in October 2015, mandates effective password management and hygiene for government entities.

The Government also supports the creation of cybersecurity standards to protect its constituents. For example, NIST 800-53 requires federal agencies to have strong controls in place to protect passwords currently being used and ensure employees are using strong passwords. Federal agencies are required to comply with these standards, as directed by The Federal Information Security Management Act.

Protecting Government Assets

The largest security gap within government agencies can be quickly and cost effectively closed with strong password policies enforced with an easy-to-use, intuitive password management solution.

Keeper is the trusted leader in password management helping organizations manage, secure and enforce strong passwords across all employee logins, applications and sites. Administrators can access Keeper natively on all mobile devices, desktops and browsers.

AES-256 bit Encryption
Keeper is a zero-knowledge password management solution. This means all information that is stored in Keeper is only accessible by the end-user. All encryption and decryption is done on-the-fly in the client's device, and the data is encrypted both in-transit (TLS) and at rest (AES-256) on Keeper's Infrastructure. Keeper is fanatical about protecting customer data, but in the unlikely event Keeper was hacked, the attackers could only possibly access the ciphertext.

Share Your Passwords Securely
Each user has a 2048-bit RSA key pair that is used for sharing password records and messages between users. Shared information is encrypted with the recipient's public key. Keeper's record sharing methodology is easy to use, secure and intuitive.

Secure More Than Passwords
Keeper protects your sensitive files, documents, digital certificates, private keys, photos and videos in a highly-secure, encrypted digital vault. You can securely share files with colleagues and have confidence knowing that your information is backed up in the Keeper Vault.

Reduce Costs and Improve Productivity With Keeper
Password resets are a major burden on the productivity of IT departments. The #1 help desk call is for a forgotten password - Forrester reports that several large organizations have allocated over $1 million annually or password-related support. This doesn't count employee frustration and productivity losses.

World Class Customer Support
All Keeper users have 24x7 access to Keeper's dedicated customer care team.

SOC 1

SOC 2

ISO27001

SOC 3

TRUSTe

PCI DSS

FISMA

Keeper enables government agencies to take control of their passwords. Every employee is provided a secure, digital vault that stores passwords and any other critical information such as encryption keys and digital certificates. Keeper will generate strong, random passwords and automatically fill them for users.

Keeper is FEDRAMP Authorized & available through ALINEDS for TEXAS Local and States Agencies

FedRAMP

ALINEDS

CENTRAL HEALTH

Keeper is Used by Local, State and Federal Agencies

More than 7,000 organizations trust Keeper including many local, state and federal government agencies. Keeper is honored to have as a customer the U.S. Federal District Courts of the Western District of Arkansas, Vermont, Eastern District of New York, Southern District of Ohio and Middle District of Louisiana.

U.S. Federal District Courts of the Middle District of Louisiana

U.S. Federal District Courts of the Eastern District of New York

U.S. Federal District Courts of Vermont

U.S. Federal District Courts of the Southern District of Ohio

U.S. Federal District Courts of the Western District of Arkansas

Recent Awards and Recognition

Keeper is honored to be recognized by these popular industry organizations.

App Store	Google Play	G2 Crowd	PCMag
Top-Rated Productivity	**Editor's Choice**	**Spring 2019 Enterprise Leader**	**Editor's Choice**
4.9 out of 5 stars	4.5 out of 5 stars	4.7 out of 5 stars	4.5 out of 5 stars

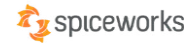| Gartner peerinsights	Trustpilot	GetApp	spiceworks
4.7 out of 5 stars	9.3 out of 10 stars	4.8 out of 5 stars	5 out of 5 stars

Sources

1 "2018 Thales Data Threat Report - Federal Edition." Thales Security
2 Hacking of Government Computers Exposed 21.5 million People." New York Times
3 "2017 U.S. State and Federal Government Cybersecurity Report." SecurityScorecard
4 "Verizon Data Breach Investigation Report 2017." Verizon
5 "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." White House

Business Sales

Federal PoC
(512) 522 1605
Dave Marshall

Texas State PoC
(737) 232 9124
Davids Achonu

www.alineds.com   info@alineds.com
www.keepersecurity.com