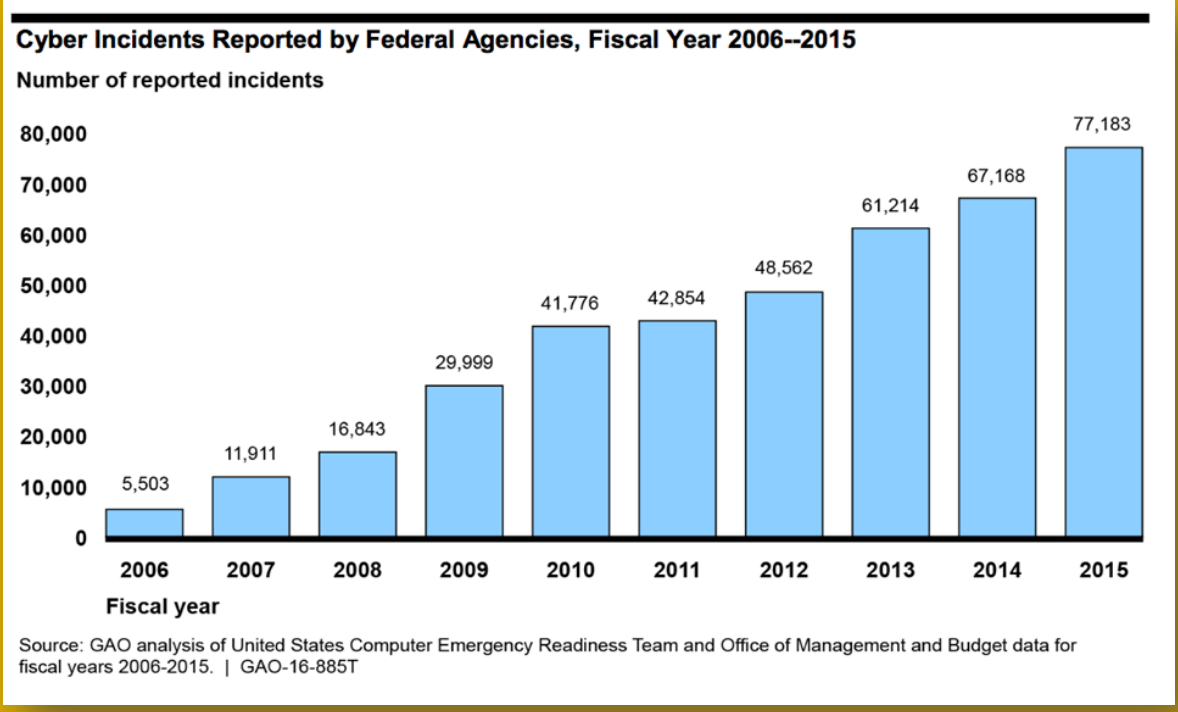
NATIONAL GOVERNMENT

Central Government Department and Agencies are the targets of an accelerating and full range of cyber attacks. Adversaries include hackers, hacktivists, malicious insiders, nation state actors, criminals, organized crime, and terrorists. Their tools range from bots and "copy from the web" scripts to sophisticated zero day vulnerabilities. And their impact can be severely damaging both to agencies' ability to operate and public confidence in government. This is a big challenge because of the huge volume of threats that agencies face on a daily basis and the scale of the potential consequences if successful. The scale of the data sets held by government, and their significance for adversaries, was illustrated by the theft of over 22 million federal employees' background investigation records from the US Office for Public Management.

Government information security leaders have to operate in a complex environment of numerous systems, aging infrastructure, skill shortages and funding constraints. They are also required by law to keep data for long periods, in the case of Archives for hundreds of years. STASH is a key partner for government to keep data securely stored and shared. Its focus on keeping the treasured data secure and resilient significantly reduces the risks inherent in defending complex and aging systems. STASH's unique authentication and encryption processes slash the risk of insider access to key data. Its secure data repositories are not vulnerable to ransomware. STASH has developed trustworthy digital repository technology and processes to ensure the storage and retrieval of viable data over many decades. STASH is an essential partner for the data integrity challenges of the government sector.



+1 (844) 833-7373
Stash America LLC
contact@stash.global

"As computer technology has advanced, federal agencies have become dependent on computerized information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Virtually all federal operations are supported by computer systems and electronic

data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, ineffective controls can result in significant risk to a broad array of government operations and assets. For example:…

- Sensitive information, such as intellectual property and national security data, and personally identifiable information, such as taxpayer data, Social Security records, and medical records, could be inappropriately added to, deleted, read, copied, disclosed, or modified for purposes such as espionage, identity theft, or other types of crime.
- Critical operations, such as those supporting national defense and emergency services, could be disrupted.
- Data could be modified or destroyed for purposes of fraud or disruption.
- Entity missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their responsibilities."

– Statement of Gregory C. Wilshusen, Director, Information Security Issues United States Government Accountability Office, Testimony to the President's Commission on Enhancing National Cybersecurity 2017

Whether you want to keep things to yourself or share with others, STASH delivers DSECaaS™ (data- security-as-a-service) to meet your needs. In a world of Open Networks and Bring Your Own Device, we focus on the crown jewels. On the data. On what really matters to your business.

STASH Data Protection for everyday valuable data and STASH HIBERNATE® for very long term data protection with data integrity for decades are the most impactful encryption and privacy Solutions ever developed to protect the actual data bytes themselves. STASH doesn't analyze, predict, try to defend, or react to data compromise after the fact like 99.99% of all other security options. When data is protected with STASH, it has a statistical probability of nil to breach, manipulation, loss, harm, or ransomware.

Data, network, and infrastructure agnostic, STASH is completely automated and simple to deploy, without changing anything about how you do business. Activated via SAAS, Secure Backup, & API