# INSIDE JOB:
## The Federal Insider Threat Report

Underwritten by Symantec

Addressing data breaches and cyber incidents perpetrated by insiders – whether malicious or unintentional – is a mounting problem. What can agencies do to minimize this significant risk?

### Agencies are struggling to combat insider threats

In the last year

**45%** of agencies have been a target of an insider threat

And nearly **one** in **three** have lost data to an insider incident

### But are making the effort to minimize incidents

**75%** are more focused on combating insider threats today than one year ago

**51%** are running mock attacks to better understand unintentional threat risks

**73%** are offering annual online training

### However, basic security measures are overlooked...

Just **39%** offer in-person security training

More than **40%** cannot tell the moment a document has been shared or how

### ...And fewer than half are employing key technologies agency-wide

**48%** Data loss prevention

**46%** Two-factor authentication

**40%** Endpoint encryption

### ...And employees are putting agencies at significant risk

**65%** say it's **common for employees** to email documents to personal accounts

**51%** say it's **common for employees** to not follow appropriate protocols

**40%** say **unauthorized employees** access government information they shouldn't at least once weekly

### Is there a holistic solution?

- Start with formal insider threat programs to leverage cyber intelligence
- Scale up training and technology – limit access points, upgrade encryption, and adopt two-factor authentication – to improve security habits
- Leverage government momentum, like Presidential CAP goals, to enhance security culture

The consequences are real – it's time for agencies to go "all in" on defending against insider threats.

To download the full report, please visit:
**www.meritalk.com/insidejob**