DOE SBIR/STTR CYBERSECURITY SERIES

FY 2025 Phase II Release 2 Applied Offices

VIDEO 6 OF 8

Secure Data: Email Security and Encryption

TOPIC

Protecting company email from spoofing and phishing, and encrypting sensitive data at rest and in transit

Practices 2.3 and 2.4 · Tier 2

Please send your Questions/Feedback to csduediligence@doe.gov

Email and Data Are Prime Targets

WHY IT MATTERS

01

Spoofing

Criminals send email that looks like it came from your company's domain.

02

Business email compromise

Fake invoices and payment-change requests from real or look-alike accounts.

03

Lost devices and interception

An unencrypted laptop or connection can expose research, IP, and CUI.

Enable Email Security

TIER 2 · PRACTICE 2.3

WHAT IT MEANS

Protect company email from spoofing, phishing, interception, malicious content, and account takeover.

HOW TO DO IT

1. Make sure STARTTLS is enabled for your company email (it may already be on)
2. Set up SPF and DKIM, and turn on DMARC with a policy of reject
3. Require MFA for email, and turn on anti-spam, anti-phishing, anti-malware, link, and attachment protection
4. Send sensitive information with encryption or an approved secure-sharing method
5. Log and watch email security events, investigate anything suspicious, and train users to report phishing

More detail: DOE SBIR/STTR Tier 2 Supplemental Guide, section 2.0 Secure Data

SPF, DKIM, and DMARC Explained

PRACTICE 2.3 · IN PLAIN ENGLISH

01

SPF

A published list of the mail servers allowed to send email for your domain.

02

DKIM

A digital signature that proves a message came from you and wasn't changed.

03

DMARC

Tells other mail systems what to do with messages that fail those checks.

04

Start, then enforce

Start DMARC in monitoring mode, review reports, then move to reject once real senders are known.

Important: SPF, DKIM, and DMARC don't replace MFA, malware filtering, user training, or encryption for sensitive data.

Utilize Strong Encryption

TIER 2 · PRACTICE 2.4

WHAT IT MEANS

Use strong encryption to protect federally funded R&D, intellectual property, credentials, CUI, and other sensitive information, both when it's stored and when it's sent.

HOW TO DO IT

1. Identify the sensitive data and file types that need protection, and where they're stored and sent
2. Encrypt laptops, mobile devices, servers, cloud storage, removable media, databases, and backups with sensitive data
3. Use secure connections (HTTPS/TLS, SSH, SFTP, secure VPN) on public networks; turn off old protocols and weak ciphers
4. Never store passwords in plain text; use approved password management
5. Protect encryption keys: limit access, and retire or rotate keys as needed
6. For CUI, use FIPS-validated encryption (NIST SP 800-171 Rev. 3, 03.13.11) and verify your cloud provider's encryption

More detail: DOE SBIR/STTR Tier 2 Supplemental Guide, section 2.4

Data at Rest and Data in Transit

PRACTICE 2.4 · TWO KINDS OF PROTECTION

AT REST

Stored data

Laptops, phones, servers, cloud storage, USB drives, databases, and backups. Use device encryption such as BitLocker and your provider's encryption features.

IN TRANSIT

Data on the move

Data crossing public or untrusted networks. Use HTTPS/TLS, SSH, SFTP, or an approved VPN, and turn off obsolete protocols.

Can a Third-Party Service Provider Help?

PRACTICES 2.3 & 2.4 · GETTING HELP

SERVICE	EMAIL SECURITY (2.3)	ENCRYPTION (2.4)
Microsoft	MFA/Conditional Access, SPF, DKIM, DMARC, Exchange Online Protection and Defender, audit and sign-in logs.	BitLocker/device encryption, Microsoft 365 and Azure encryption, Key Vault for managed keys.
Google	2-Step Verification, SPF, DKIM, DMARC, Gmail spam and phishing protection, email log search.	Built-in encryption and secure transport; Cloud KMS/CMEK in Google Cloud.
AWS / MSP	An MSP or email-security provider can set DNS records, filtering, and alerts. Keep admin visibility.	AWS encryption at rest (S3, EBS, RDS), TLS in transit, AWS KMS for keys.

For CUI, a provider saying 'data is encrypted' isn't enough evidence. Verify the specific service, configuration, and contract requirements.

What Happens If You Skip These Practices

WHAT HAPPENS IF YOU DON'T

To your business

- Criminals send convincing email that appears to come from you.
- Fake invoices and payment-change requests lead to lost money.
- A lost, unencrypted laptop becomes a data breach.
- Sensitive research or CUI is exposed in transit.

To your DOE SBIR/STTR award

- Gaps can come to light during a DOE on-site review or audit.
- You won't have the evidence the form says you can produce.
- Your signed Management Review would describe practices that aren't really in place.

What to Show DOE for Each Practice

EVIDENCE TO KEEP READY

PRACTICE	EVIDENCE (FROM THE EVIDENCE FORM)
2.3 Email security	Email process and/or policy
2.4 Strong encryption	Encryption policy and/or process for identifying data at rest and in transit

Guide estimates: email 2–4 hours (up to 1–3 days with DNS changes); encryption 2–6 hours (1–3 days for servers, media, or FIPS checks).

Remember These

KEY TAKEAWAYS

1. Turn on SPF, DKIM, and DMARC set to reject
2. Use your email platform's built-in protections, plus MFA
3. Encrypt sensitive data at rest and in transit
4. For CUI, use FIPS-validated encryption and verify your providers

Up next · Video 7: Unsuccessful-Login Monitoring: Stop Password Guessing

Please send your Questions/Feedback to csduediligence@doe.gov