
DOE SBIR/STTR CYBERSECURITY SERIES
FY 2025 Phase II Release 2 Applied Offices
VIDEO 8 OF 8

Incident Response: Your Plan and Procedures

TOPIC

Writing a short, usable incident response plan and step-by-step procedures your team can follow

Practices 2.6 and 2.7 · Tier 2

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



Plan for a Bad Day Before It Happens

WHY IT MATTERS

01

Ransomware and malware

Systems are locked or infected, and research stops.

02

Phishing and account takeover

Someone gets into email or cloud accounts.

03

Lost or stolen equipment

A laptop disappears with research data on it.

04

Unauthorized disclosure

R&D data, IP, or CUI leaks, including through insiders.



Establish and Maintain an Incident Response Plan

TIER 2 • PRACTICE 2.6

WHAT IT MEANS

Keep a short, usable plan for responding to cyber incidents that affect your systems, federally funded R&D, intellectual property, sensitive information, and CUI.

HOW TO DO IT

- 1 Write a plan for likely events: phishing, ransomware, lost devices, R&D disclosure, cloud compromise, insiders, internet-facing attacks
- 2 Assign roles: leadership, technical investigation, communications, legal/contract reporting, recovery, and MSP/MSSP coordination
- 3 Keep internal and external contacts, and define severity levels and when to escalate
- 4 Cover containment, evidence preservation, recovery, communications, and reporting at a high level
- 5 Practice the plan at least yearly, and update it after exercises, incidents, and major changes

More detail: DOE SBIR/STTR Tier 2 Supplemental Guide, section 4.0 Incident Response



A Plan People Can Actually Use

PRACTICE 2.6 • KEEP IT USABLE

01

Keep it short

A practical 3–8 page plan with current contacts, roles, reporting triggers, and recovery actions beats a long document.

02

Know who to call

Internal contacts, MSP/MSSP, cyber insurer, legal counsel, cloud providers, and the DOE SBIR/STTR reporting contact.

03

Report to DOE

DOE SBIR/STTR incident-reporting email: csduediligence@doe.gov. Follow the timeframes in your award and current DOE instructions.



Maintain Incident Response Procedures

TIER 2 • PRACTICE 2.7

WHAT IT MEANS

Keep repeatable, step-by-step procedures your people can follow when a cyber incident is suspected or confirmed.

HOW TO DO IT

- 1 Follow a simple flow: Report, Assess, Contain, Preserve, Eradicate, Recover, Notify, Document, Improve
- 2 Tell employees exactly who to contact, with a backup method if email or systems are down
- 3 Define what employees do right away; only people assigned to investigate should investigate
- 4 Assess what happened, when, what's affected, whether R&D or CUI is involved, and how serious it is
- 5 Decide who makes outside reporting decisions and how you coordinate with DOE SBIR/STTR, providers, and partners
- 6 Practice with a tabletop walkthrough, and update based on lessons learned

More detail: DOE SBIR/STTR Tier 2 Supplemental Guide, section 2.7



Nine Steps from Report to Improve

PRACTICE 2.7 • INCIDENT RESPONSE PROCEDURE WORKSHEET

01

Report

How people report, with primary and backup contacts.

02

Assess

What, when, what's affected, how severe, R&D or CUI?

03

Contain

Isolate devices, disable accounts, block traffic.

04

Preserve

Keep logs, email, screenshots, files, timestamps.

05

Eradicate

Remove malware, bad access, exposed credentials.

06

Recover

Restore from known-good sources and monitor.

07

Notify

Decide on outside reporting; contact DOE and others.

08

Document and close

Record facts, decisions, actions, and outcome.

09

Improve

Update safeguards, training, and the plan.



Four Rules During an Incident

PRACTICE 2.7 • FOR EVERY EMPLOYEE

01

Report right away

Contact the named person immediately, even if you're not sure.

02

Use the backup channel

If email or systems are down or compromised, use the agreed alternative.

03

Don't investigate alone

Leave investigation to the people assigned to it.

04

Don't delete anything

Stop using the suspicious message or file, but keep it. It's evidence.



Can a Third-Party Service Provider Help?

PRACTICES 2.6 & 2.7 • GETTING HELP

SERVICE	HOW IT CAN HELP
Microsoft 365 / Azure	Security portals give alerts, logs, account and device actions, endpoint isolation where licensed, and evidence exports.
Google Workspace / Google Cloud	Security investigation and audit tools, account suspension and session reset, and cloud logging.
MSP / MSSP / cyber insurer	24/7 monitoring, investigation, containment, and recovery support, if it's in the contract. Write down what they do and how to reach them.

Your company keeps its own roles, reporting duties, and plan. Your procedures should say what employees do first, how the provider is contacted, and what authority the provider has.

What Happens If You Skip These Practices

WHAT HAPPENS IF YOU DON'T

To your business

- Confusion and delay make incidents bigger and more expensive.
- Evidence gets destroyed before anyone can investigate.
- Required notifications to DOE and others can be missed.
- Loss of intellectual property can harm your business.

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)
2.6 Incident response plan	Approved incident response plan (template provided by SBIR/STTR Office)
2.7 Incident response procedures	Approved incident response procedure worksheet (template provided by SBIR/STTR Office)

Guide estimates: plan 3–6 hours (1–2 business days with several sites or providers); procedures 4–8 hours (1–3 business days with separate playbooks).



Remember These

KEY TAKEAWAYS

- 1 Write a short plan with roles, contacts, and when to escalate
- 2 Turn it into step-by-step procedures everyone can follow
- 3 Report incidents to DOE SBIR/STTR at csduediligence@doe.gov
- 4 Practice at least once a year, and update after every incident

Series complete • Thank you for watching

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

