Four Inc. New Hire IT Training

Agenda

- Importance of IT compliance
- Employee responsibilities to maintain a quality IT plan
- Federal regulations
- Policy overview & action items

Purpose

Why does IT security matter?

- Mandatory per internal policies
- Reputation within the industry
- Audits
  - Recent GSA SCRM audit required proof of our enacted policies
  - CMMC audit
    - Lv 2 in Sept of 2026
- Aligns with future business contracts and growth
  - CMMC and other regulations in the future may require strict IT standard

Change Control Board (CCB)

- Approves changes to IT systems
- Coordinates and provides oversight for changes related to security and operations

- CCB members:

  David Stewart (CEO)
  Bree Burk (VP of Operations)
  Michael Lucas (Director of Programs and compliance)

ACS Services

ACS

- Manages devices, server, application issues, etc.
- Can be reached by phone or email for helpdesk support
- ***Help Desk Support***
  - **Email:** helpdesk@acs.com
  - **Phone:** 617-960-9850

24x7 Support

Technology breaks. Urgent IT issues happen. The team at ACS is here to help when you need it, 24/7.

IT Team

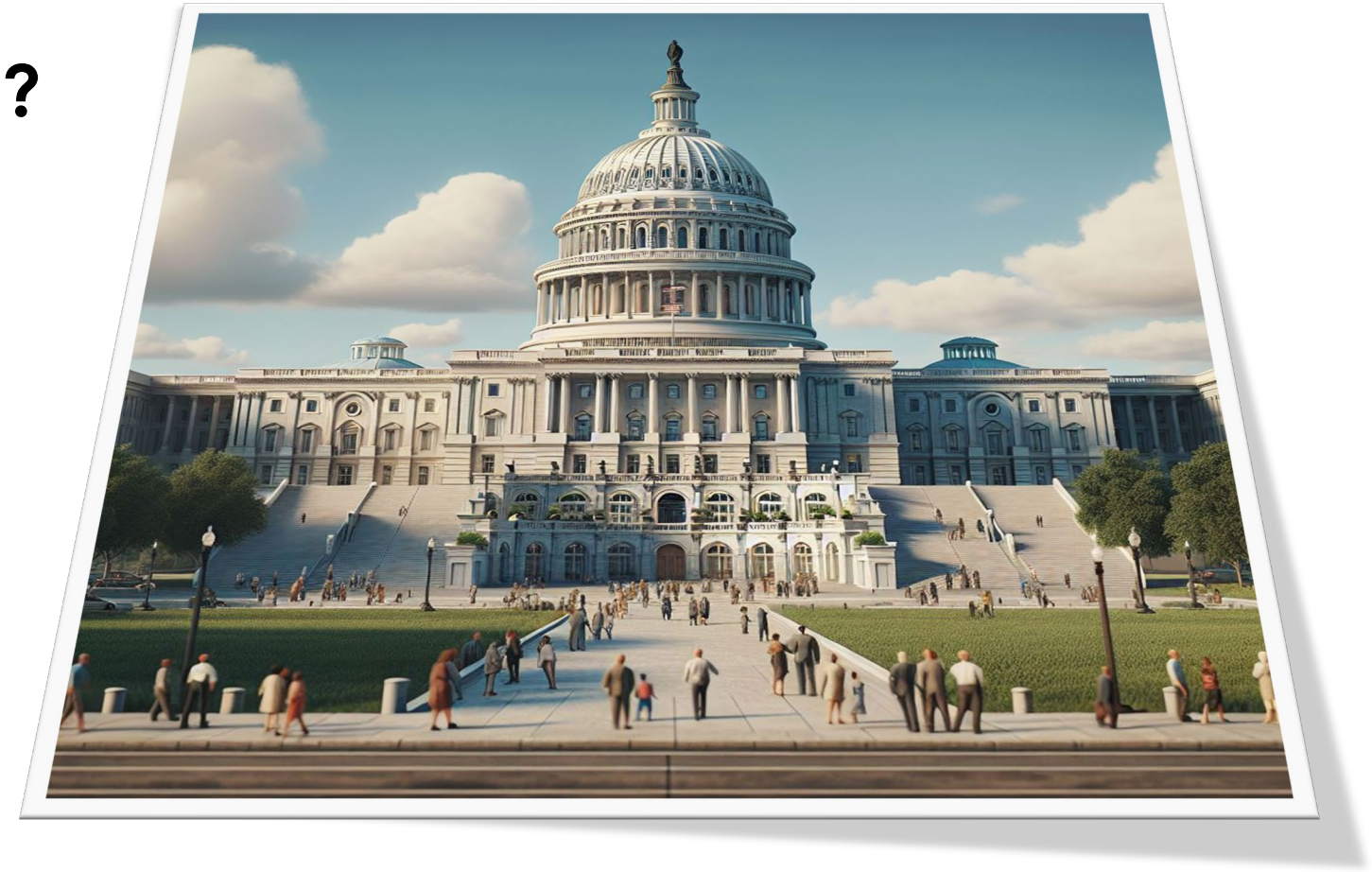
Internal Team

- Bree Burk
- Michael Lucas
- Cody Powers
- ACS

Federal Regulations

What are they?
Who does this apply to?
Why do we care?

- NIST 800-171
- CMMC



NIST

NIST Special Publication 800-171

(National Institute of Standards and Technology)

Official purpose: to help organizations protect Controlled Unclassified Information (CUI)

Involves:

- Access Control
- Configuration Management
- Incident Response
- Audit and Accountability

Integration with CMMC: NIST 800-171 serves as a foundational reference for CMMC, where compliance with NIST requirements is necessary for CMMC certification

CMMC

Cybersecurity Maturity Model Certification (CMMC)

Official purpose:
CMMC regulations aim to enhance cybersecurity practices among organizations working with the Department of Defense (DoD).

Will appear via a DFARS 7021 clause in contract solicitations & awards

Certification Requirement:
Measured and managed by "controls". Level 2 contains 110 controls with 320 objectives.

Dec 16th, 2024 implementation
We achieved Lv 1 on Sept. 30, 2025

CMMC

What if we do not pursue CMMC?

Loss of Contracts:
Organizations that do not achieve the required CMMC certification may be ineligible to bid on or *maintain* contracts with the Department of Defense (DoD)*.

- *Initially limited to the DoD, but now expanding to FAR, Civ & DHS

CMMC

Your responsibility

Customers will be seeking CMMC certification and may ask you about our CMMC plan

Four Inc is positioned as an educator for CMMC in the Federal space

Four Inc achieved CMMC Lv. 1- currently seeking CMMC Lv. 2

Everyone in the deal flow needs CMMC certification

Sales reps will need to know how more info about how to communicate with vendors regarding CMMC

FCI and CUI

What is FCI?

► "Federal Contract Information (FCI) is any information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government."

It does **not** include information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Key Regulation:

► **FAR 52.204-21** – Basic Safeguarding of Covered Contractor Information Systems

This clause requires contractors to apply **15 basic safeguarding requirements** to protect FCI on covered contractor information systems.

FCI and CUI

What is CUI?

► "Controlled Unclassified Information(CUI) is information that requires safeguarding, or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, but is not "classified""

- It is determined by the contracting officer at time of award.

Note: This clause is not applicable to contractors when it has been determined that CUI is neither managed nor stored in the contractor's environment.

Policy Overview and Action Items

Identifying and Avoiding Phishing Attacks

FOUR inc.

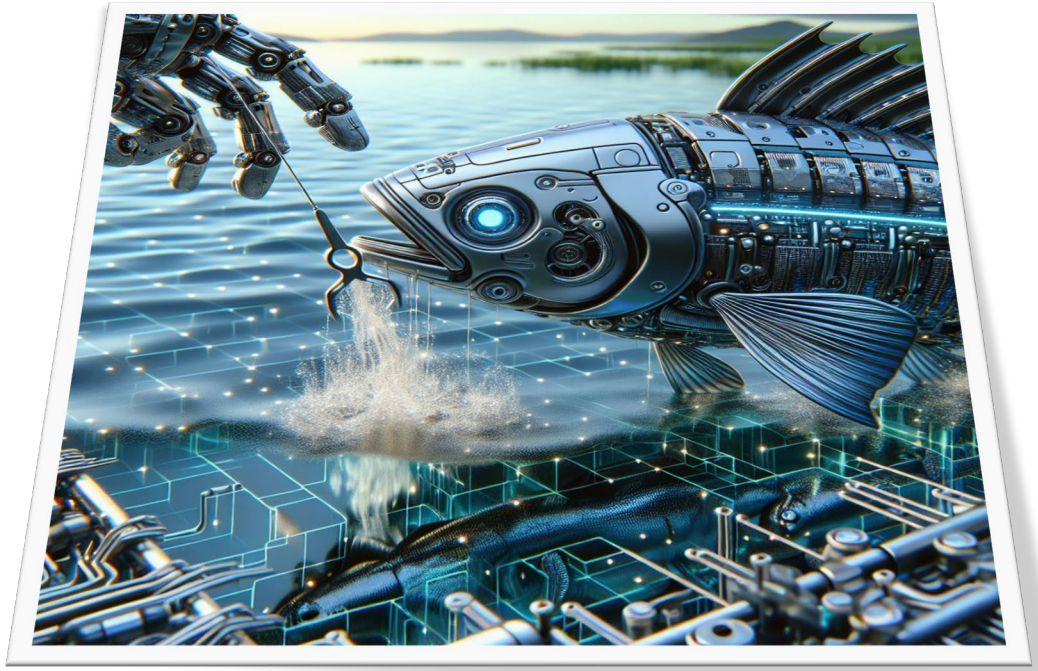
Phishing is a cybercrime where attackers attempt to trick individuals into providing sensitive information

Dangers of Phishing

Data Theft:
Successful phishing can lead to identity theft, financial loss, and unauthorized access to accounts.

Malware Infection: Some phishing involves attachments that install malware on your device

Reputation Damage: Businesses can suffer from loss of customer trust and brand reputation



Identifying and Avoiding Phishing Attacks

Be Skeptical: Verify the source of emails, texts, or calls requesting sensitive information.

Check URLs Carefully: Look for misspellings or unusual domain names in links. Hover over links to see the actual URL before clicking.

Report Phishing Attempts: If you receive a phishing email or message, report it to the IT Team (Michael Lucas or Cody Powers) or ACS Services.

Action: Educate Yourself and Others: Stay informed about common phishing tactics and share knowledge with your colleagues to help them recognize potential threats

Security Awareness Training

Employees must:

- Complete **10/12 Monthly IT Trainings** on Huntress
- These will be emailed to you in the first week of the month

The training will cover topics such as:

- Identifying and avoiding phishing/social engineering attacks
- Proper handling and protection of sensitive data
- Physical security practices
- Incident reporting procedure

<u>Action: Complete Monthly security videos</u>

Physical Security Practices - External

Sign-in Requirements

- Four Inc. requires all visitors to sign in at the reception desk upon arriving at Four Inc.

Visitor Access

- Visitors must only be given access to the Four Inc. premises that is appropriate to the reason for their visit.
- Visitors must be escorted through HQ unless they are considered "trusted" by Four Inc. (i.e., building custodial staff, a trusted contractor, etc.)

Physical Security Practices - Internal

FOUR inc.

Clean desk policy

- Remove sensitive data from desk
- Close or lock computers if stepping away for an extended amount of time
- Put away documents if you have them sitting out

Incident reporting procedures

<u>Cybersecurity incidents must be reported to the IT team.</u>

Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.)
- Suspected virus/malware
- Loss or theft of any device that contains company information
- Loss or theft of keycard
- Any other suspicious event that may impact Four Inc.'s information security

If a security incident or breach of policy is discovered or suspected, the user must immediately notify the IT team at: securityincidents@fourinc.com

Acceptable Use Policy

Protect Company Data: Use company systems only for authorized business purposes. Always safeguard confidential and sensitive information.

Responsible Technology Use: Do not install unapproved applications or bypass security controls.

Professional Communication: Use email, messaging, and collaboration tools respectfully and professionally.

Prohibited Online Activities: Employees must not use work devices to search for or access content related to illegal activities, sexual material, gambling, discriminatory content, or hate-based content.

Monitoring and Compliance: Company systems may be monitored to ensure compliance. Violations may result in disciplinary action.

iBoss

iBoss is a cybersecurity tool that combines VPN and other Zero Trust Network Access (ZTNA) structures to securely connect users to the internet.

- All activity is verified and filtered, **so even if you're on an untrusted network,** threats are blocked before they reach your device.

- iBoss is **always on.** You don't need to launch it or adjust it.

- You can connect to **ANY Wi-Fi as long as iBoss is active.**

Mobile Data Storage

Storage of company data is prohibited* on-

- Flash Drives
- Personal computers
- External hard drives
- Any other personal data storage device

***Exceptions can occur with written approval by a member of the CCB**

Component Disposal

Component Disposal (STD SR-12)

- Documents are removed and stored by **IronMountain**
- Documents containing CUI or contractual data must be retained for at least seven years before destruction

Action: When devices or technology breaks, give it to the IT team and we will give it to ACS and get a POD (proof of destruction)

Questions/Answers

Questions?