Incrypt Cyber

SECURE BEHAVIOR & COMPLIANCE

GOVERNMENT & REMOTE WORKFORCE

Verified alignment: NIST CSF 2.0, FISMA /NIST SP 800-53 Rev. 5, CISA Cyber Essentials

For education purposes only

Presented by Juliet Roberts, BAT in Cybersecurity, Cybersecurity & AI Risk Consultant

01 July 2025

Daily Secure Practice and Compliance Checklist

Verified alignment with NIST CSF 2.0, FISMA /NIST SP 800-53 Rev. 5, CISA Cyber Essentials for education use only.

- **Lock your screen**: When away from your device, ensure your screen is locked to prevent unauthorized access.
- **Use unique, complex passwords**: For every account, create unique and complex passwords or pass-phrases to enhance security.
- **Enable multi-factor authentication (MFA)**: Implement MFA on all work platforms to add an extra layer of security.
- **Avoid using personal email or devices**: Refrain from using or devices for work-related tasks.
- **Verify links and sender addresses**: Before clicking or responding to emails, verify the links and sender addresses to ensure authenticity.
- **Avoid public Wi-Fi**: Unless connected through a government approved VPN, avoid using public Wi-Fi networks.
- **Regular software updates**: Updates your software, browsers, and security tools regularly to ensure the latest security patches and updates.
- **Report suspicious emails or system activity**: Immediately report suspicious emails or system activity to your security team.
- **Refrain from sharing passwords or credentials**: Never share your passwords or credentials, even with colleagues.
- **Backup critical data**: Backup critical data in accordance with agency or company policy to ensure data integrity and availability.

Protecting Government Data:

- **Handle controlled Unclassified Information (CUI) or sensitive data:** Only handle controlled unclassified information (CUI) or sensitive data in approved systems.
- **Adhere to agency guidelines:** Follow agency guidelines for storage, encryption, and disposal of official records.

Accessibility for Remote Users:

- **Use screen reader-compatible platforms:** Utilize screen reader-compatible platforms and mobile devices protections when working on the go to enhance accessibility for remote users.
- **Ensure proper device lock settings and MFA apps :** Ensure that your device lock settings and MFA apps function properly on remote connections.

Role-Based Awareness Tips

These practices support different roles in achieving NIST CSF aligned security

Frontline Staff (Aligned with PR.AT, PR.AC,DE.CM):

- Follow approved login procedures (PR.AC-1).
- Participate in all required security trainings (PR.AT-1).
- Report incidents quickly (RS.AN-1 / DE.CM-3).

IT & Admin Roles (Aligned with PR.IP, DE.CM, ID.GV):

- Maintain system logging and endpoint detection (DE.CM-3 / DE.CM-7).
- Review and respond to audit reports (ID.GV-2/ ID.RA-3).
- Ensure endpoint protection policies are consistently enforced (PR.IP-3 / PR.PT-4).

Leadership and Managers (Aligned with ID.GV,ID.RA, GV.RR)

- Promotes a culture of cybersecurity throughout the organization (GV.RR-1)
- Support regular risk assessments and tabletop exercises (ID.RA-1).
- Approve funding and policy updates for security initiatives (ID.GV.2 / GV.OV-3).

Framework Compliance Reference

This checklist and secure practice guide aligned with:

- NIST Cybersecurity Framework 2.0 (NIST CSF 2.0)
- FISMA (Federal Information Security Modernization Act / NIST 800-53 Rev.5)
- CISA Cyber Essentials (#1 - Yourself (leadership responsibility, culture of cybersecurity), #2 - Your staff (security awareness), #3 - Your data (CUI handling, encryption, data backup), #4 - Your surroundings (devices locking, VPN usage, remote work safeguards)) supporting day-to-day behavior across roles.

Verified Alignment: NIST CSF 2.0, CISA Cyber Essentials & FISMA

Training Habits	NIST CSF 2.0 Category	CISA Essentials Alignment	FISMA/NIST SP 800-53 Rev. 5 Controls
Lock your screen	PR.PT-3 - Least functionality	#4 - Your Surroundings	✅ AC-11, AC-2(5)
Use unique, complex passwords	PR.AC-1- Identify management	#2 - Your staff / #3 - Your data	✅ IA-5, AC-2
Enable multi-factor authentication (MFA)	PR.AC-7 - MFA	#2 - Your staff / #4 - Your surroundings	✅ IA-2(1), IA-(2)
Avoid using personal email or devices	PR.DS-5 / PR.AC-3 - Data-in-transit protection	#3 - Your data / #4 - Surroundings	✅ AC-19, CS-12

Verified Alignment: NIST CSF 2.0, CISA Cyber Essentials & FISMA

Training Habits	NIST CSF 2.0 Category	CISA Essentials Alignment	FISMA/NIST SP 800-53 Rev. 5 Controls
Verify links and sender addresses	DE.CM-1 / PR.AT-2	#2 - Your staff	✅ SI-4, AT-2
Avoid public Wi-FI	PR.AC-5 -Network integrity / PR.PT-4	#4 - surroundings	✅ AC-17(2), CS-12
Regular software updates	PR.IP-12 - Vulnerability management	#2 - Your staff / #3 - Your data	✅ SI-2
Report suspicious emails or system activity RS.AN-1 /RS.CO-1 #6 - Your actions ✅ IR-6, IR-8	RS.AN-1 /RS.CO-1	#6 - Your actions	✅ IR-6, IR-8

Verified Alignment: NIST CSF 2.0, CISA Cyber Essentials & FISMA

Training Habits	NIST CSF 2.0 Category	CISA Essentials Alignment	FISMA/NIST SP 800-53 Rev. 5 Controls
Refrain from sharing passwords or credentials	PR.AC-1, PR.AC-6 / PR.AT-2	#2 - Your staff / #1 - Yourself	✅ IA-5(f), AT-2(2)
Avoid public Wi-FI	PR.AC-5 -Network integrity / PR.PT-4	#4 - surroundings	✅ AC-17(2), CS-12
Regular software updates	PR.IP-12 - Vulnerability management	#2 - Your staff / #3 - Your data	✅ SI-2
Backup critical data	PR.IP-4 / PR.DS-1	#3 - Your data	✅ CP-9, CP-10

Protecting Government Data

Verified Alignment: NIST CSF 2.0 , CISA Cyber Essentials & FISMA			
Training Habits	NIST CSF 2.0 Category	CISA Essentials Alignment	FISMA/NIST SP 800-53 Rev. 5 Controls
Handle controlled Unclassified Information (CUl) in approved systems.	PR.DS-1/ ID.GV-3	#3 - Your data	✅ AC-12, SC-12, SC-28, CS-32
Follow encryption and storage guidelines	PR.DS-2 / PR.IP-4	#3 -Your data	✅ SC-12, SC-28, CS-34

Accessibility For Remote Users

Verified Alignment: NIST CSF 2.0 , CISA Cyber Essentials & FISMA			
Training Habits	NIST CSF 2.0 Category	CISA Essentials Alignment	FISMA/NIST SP 800-53 Rev. 5 Controls
Use screen-reader compatible, secured platforms	PR.IP-11 / PR.PT-1	#4 - Your surroundings	✅ AC-17(5), SC-35
Ensure device locked + MFA Functions remotely.	PR.AC-7 / PR.PT-3	#4 - Your surroundings	✅IA-2(1), AC-11, AC-19

For additional guidance visit

Source:

National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF 2.0.) (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29.
https://doi.org/10.6028/NIST.CSWP.29

CISA Cyber Essentials
https://www.CISA.gov/Cyber-Essentials

National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5).
https://doi.org/10.6028/NIST.SP.800-53r5

IncryptCyber Awareness | Powered by Incrypt Cyber LLC | Founder, Juliet Roberts | BAT Cybersecurity & Cybersecurity & AI Risk Consultant

Training content by Incrypt Cyber LLC, aligned with NIST CSF, FISMA, CISA Cyber Essentials for education use only.

🟦 Cybersecurity Framework Glossary

IncryptCyber Awareness | Aligned with Federal Standards

🧩 NIST Cybersecurity Framework 2.0 (CSF 2.0)

The NIST Cybersecurity Framework (CSF) 2.0, released in February 2024 by the National Institute of Standards and Technology (NIST), is a flexible, risk-based approach for managing cybersecurity risks across organizations of all sizes and sectors.

It defines high-level cybersecurity outcomes organized into six core functions:

1. **Govern (GV)**: Establish cybersecurity policies, roles, and oversight.
2. **Identify (ID)**: Understand assets, systems, data, and risks.
3. **Protect (PR)**: Implement safeguards to protect services and operations.
4. **Detect (DE)**: Identify potential cybersecurity events quickly.
5. **Respond (RS)**: Take action during a cybersecurity incident.
6. **Recover (RC)**: Restore services and reduce impact after incidents.

CSF 2.0 emphasizes governance, continuous improvement, and integration with enterprise risk management. It can be tailored by public and private sector organizations to strengthen their cybersecurity posture over time.

Reference: NIST Cybersecurity Framework 2.0

🏛️ FISMA via NIST SP 800-53 Revision 5

The Federal Information Security Modernization Act (FISMA) requires U.S. federal agencies and their contractors to implement and maintain security programs that protect government data and systems.

To meet FISMA requirements, agencies use NIST Special Publication 800-53 Revision 5:
Security and Privacy Controls for Information Systems and Organizations

This publication provides a detailed catalog of security and privacy controls organized by control families, including**:**

- **Access Control (AC)**
- **Incident Response (IR)**
- **System and Communications Protection (SC)**
- **Awareness and Training (AT)**
- **Audit and Accountability (AU)**

SP 800-53 Rev. 5 emphasizes control flexibility, privacy integration, and support for enterprise risk management. It is the foundational standard for securing federal information systems, including those processing Controlled Unclassified Information (CUI).

Reference**:** NIST SP 800-53 Rev. 5

🛡️ CISA Cyber Essentials

Developed by the Cybersecurity and Infrastructure Security Agency (CISA), the Cyber Essentials Toolkit is a simple, starter framework that outlines foundational actions for improving cybersecurity in smaller organizations, municipalities, and government teams.

It's organized around six key elements:

1. **Yourself –** Lead by example. Create a culture of cybersecurity.
2. **Your Staff –** Train and empower users to identify threats.
3. **Your Systems –** Secure devices, software, and networks.
4. **Your Surroundings –** Control access to physical and digital environments.
5. **Your Data –** Protect, back up, and encrypt critical information.
6. **Your Actions –** Detect incidents, respond quickly, and recover operations.

The CISA Cyber Essentials are mapped to broader frameworks like NIST CSF, making them ideal for non-technical leadership, local government, and resource-limited environments.

Reference: CISA Cyber Essentials

Incrypt Cyber

Thank you

Presented by Juliet Roberts
📞346 298 4961
✉️ info@incryptcyber.com

01 July 2025