Executive Order 14028: Improving the Nation's Cybersecurity

Signed: May 12, 2021

Federal Register Number: 86 FR 26633

Status: Active

Overview

This executive order aims to improve the nation's cybersecurity by establishing comprehensive requirements for federal agencies and contractors regarding software security, incident reporting, supply chain security, and critical infrastructure protection.

Key Provisions

Section 1: Policy

The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, private sector, and the American people's security and privacy. The Federal Government must lead by example and take bold action to improve its cybersecurity.

Section 2: Removing Barriers to Sharing Threat Information

Federal agencies shall:

- Adopt cloud technology and zero trust architecture
- Accelerate movement to secure cloud services
- Centralize and streamline access to cybersecurity data
- Enable multi-factor authentication and encryption

Section 3: Modernizing Federal Government Cybersecurity

All agencies must:

- Deploy endpoint detection and response (EDR) capabilities
- Implement enhanced logging and information sharing
- Adopt zero trust architecture principles
- Encrypt data at rest and in transit

Section 4: Cybersecurity Requirements for Federal Contractors

Contractors and service providers must:

• Share certain cyber incident and threat information

• Meet baseline cybersecurity standards

• Implement supply chain risk management

• Maintain comprehensive software bills of materials (SBOM)

Compliance Requirements for Grant Programs

Infrastructure and Technology Grants

Projects involving digital infrastructure, information systems, or technology deployment must:

1. **Cybersecurity Architecture Requirements**

• Implement zero trust architecture principles

• Deploy multi-factor authentication (MFA) for all users

• Encrypt sensitive data at rest and in transit

• Implement network segmentation

2. **Incident Response Capabilities**

• Establish incident response and recovery procedures

• Deploy endpoint detection and response (EDR) tools

• Implement security information and event management (SIEM)

• Maintain incident reporting protocols

3. **Supply Chain Security**

• Conduct supply chain risk assessments

• Obtain software bills of materials (SBOM) from vendors

• Verify security practices of third-party providers

• Document supply chain security controls

4. **Security Monitoring and Logging**

• Enable comprehensive logging across all systems

- Retain logs for minimum 90 days
- Implement real-time security monitoring
- Conduct regular security audits

Emergency Management and Public Safety Grants

Projects involving emergency communications or public safety systems must additionally:

- Ensure interoperability with federal systems
- Implement secure communications protocols
- Establish backup and redundancy systems
- Conduct regular security testing and exercises

Mandatory Security Controls

Authentication

- Multi-factor authentication required for all users
- Phishing-resistant authentication methods preferred
- Strong password policies enforced
- Regular access reviews conducted

Data Protection

- Encryption of sensitive data (AES-256 or equivalent)
- Secure data disposal procedures
- Data loss prevention (DLP) mechanisms
- Privacy impact assessments completed

Network Security

- Microsegmentation and zero trust principles
- Secure remote access (VPN with MFA)
- Regular vulnerability scanning
- Intrusion detection and prevention systems

Software Security

- Secure software development lifecycle

- Regular security patches and updates

- Software composition analysis

- Penetration testing before deployment

Grant Evaluation Criteria

Cybersecurity components will be evaluated on:

1. **Security Architecture** (35%): Comprehensiveness of security design

2. **Incident Response** (25%): Preparedness for security incidents

3. **Compliance** (20%): Adherence to federal security standards

4. **Supply Chain Security** (15%): Vendor and supply chain risk management

5. **Continuous Monitoring** (5%): Ongoing security assessment capabilities

Documentation Requirements

Applicants must provide:

- Cybersecurity architecture diagram

- Security assessment and authorization (SA&A;) plan

- Incident response plan and procedures

- Supply chain security risk assessment

- Vendor security documentation and SBOMs

- Data protection and privacy plan

- Security monitoring and logging strategy

- Disaster recovery and business continuity plan

Federal Security Standards Referenced

- **NIST Cybersecurity Framework**: Core security practices

- **NIST SP 800-53**: Security and privacy controls

- **NIST SP 800-171**: Protecting controlled unclassified information

- **FedRAMP**: Cloud security requirements

- **CISA Binding Operational Directives**: Mandatory security requirements

Incident Reporting Requirements

Grant recipients must:

- Report cyber incidents within 24 hours to CISA
- Preserve evidence for investigation
- Cooperate with federal incident response
- Implement remediation measures promptly

Training and Awareness

Projects must include:

- Cybersecurity awareness training for all personnel
- Role-based security training for system administrators
- Phishing simulation exercises
- Annual security refresher training

Exemptions and Waivers

Exemptions may be granted for:

- Legacy systems with documented compensating controls
- Projects with minimal digital components
- Circumstances where requirements are technically infeasible

Waiver requests must be submitted with detailed justification and risk assessment.

Review and Updates

Cybersecurity requirements will be reviewed:

- Annually for alignment with evolving threats
- After major cyber incidents affecting federal systems
- When new CISA directives are issued

Resources and Support

Technical Assistance Available From:

- Cybersecurity and Infrastructure Security Agency (CISA)
- National Institute of Standards and Technology (NIST)
- Department of Homeland Security (DHS)
- Agency chief information security officers (CISOs)

Key Contacts:

- CISA Central: [email protected]
- Incident Reporting: [email protected]
- Technical Support: Federal Cybersecurity Technical Assistance

Common Compliance Pitfalls to Avoid

- Insufficient logging and monitoring capabilities
- Weak authentication mechanisms (password-only access)
- Inadequate supply chain security documentation
- Missing incident response procedures
- Lack of encryption for sensitive data
- Failure to maintain SBOMs
- Inadequate security testing

Success Criteria

A compliant project will demonstrate:

- Comprehensive security architecture aligned with zero trust principles
- Robust incident detection and response capabilities
- Verified supply chain security controls
- Continuous security monitoring and improvement
- Well-trained personnel aware of security responsibilities

Implementation Date: June 12, 2021

Phased Implementation: Some requirements have extended timelines

Compliance Verification: Regular audits and assessments required

This executive order establishes a new baseline for federal cybersecurity. Grant projects involving digital infrastructure or technology must meet these requirements to ensure the security and resilience of federally funded systems.

Questions? Contact your agency's cybersecurity compliance office or CISA for guidance on specific requirements.