SCF Domain Controls per SCF Assessment

Each Security Assessment uses *SCF Control Questions* from the Domains and Controls below, see full list at https://www.securecontrolsframework.com/ It is strongly recommended that organizations perform a full assessment using all 1000 SCF Security Control Questions, please review the ICM Overview for more info.

SCF Domain	SCF 15 Security Assessment	SCF 50 Security Assessment	SCF 250 Security Assessment
Security & Privacy Governance	• Publishing Security & Privacy Documentation	• Publishing Security & Privacy Documentation	• Publishing Security & Privacy Documentation • Periodic Review & Update of Security & Privacy Program
Asset Management	• Secure Disposal, Destruction or Re-Use of Equipment	• Asset Inventories • Software Licensing Restrictions • Secure Disposal, Destruction or Re-Use of Equipment • Return of Assets • Bring Your Own Device (BYOD) Usage • Decommissioning	• Asset Governance • Asset Inventories • Automated Unauthorized Component Detection • Software Licensing Restrictions • Secure Disposal, Destruction or Re-Use of Equipment • Return of Assets • Bring Your Own Device (BYOD) Usage • Decommissioning
Business Continuity & Disaster Recovery	• Data Backups	• Data Backups	• Data Backups • Testing for Reliability & Integrity • Cryptographic Protection • Information System Recovery & Reconstitution • Backup & Restoration Hardware Protection • Isolated Recovery Environment

Capacity & Performance Planning			
Change Management			• Stakeholder Notification of Changes
Cloud Security			• Sensitive Data In Public Cloud Providers
Compliance		• Statutory, Regulatory & Contractual Compliance • Security Assessments	• Statutory, Regulatory & Contractual Compliance • Security Assessments
Configuration Management		• User-Installed Software	• System Hardening Through Baseline Configurations • Reviews & Updates • Respond To Unauthorized Changes • Periodic Review • Unauthorized or Authorized Software (Blacklisting or Whitelisting) • Unsupported Internet Browsers & Email Clients • User-Installed Software • Unauthorized Installation Alerts
Continuous Monitoring		• Centralized Collection of Security Event Logs • Monitoring for Indicators of Compromise (IOC)	• Continuous Monitoring • Reviews & Updates • Automated Response to Suspicious Events • Automated Alerts • Centralized Collection of Security Event Logs • Correlate Monitoring Information • System-Wide / Time-Correlated Audit Trail • Content of Audit Records • Privileged Functions Logging

			• Monitoring Reporting • Monitoring For Information Disclosure • Monitoring for Indicators of Compromise (IOC) • Anomalous Behavior • Unauthorized Activities
Cryptographic Protections	• Encrypting Data At Rest	• Encrypting Data At Rest	• Use of Cryptographic Controls • Transmission Confidentiality • Encrypting Data At Rest • Storage Media • Database Encryption • Non-Console Administrative Access • Wireless Access Authentication & Encryption
Data Classification & Handling	• Ad-Hoc Transfers	• Media Sanitization Documentation • Ad-Hoc Transfers • Information Disposal	• Data Protection • Data Stewardship • Media Access • Disclosure of Information • Sensitive Data Inventories • Periodic Scans for Sensitive Data • Physical Media Disposal • Digital Media Sanitization • Media Sanitization Documentation • Limits of Authorized Use • Protecting Sensitive Data on External Systems • Information Sharing • Transfer Authorizations • Data Access Mapping • Data Mining Protection • Ad-Hoc Transfers • Media & Data Retention • Information Disposal • Personal Data (PD) Collection

Embedded Technology			
Endpoint Security	• Malicious Code Protection (Anti-Malware) • Phishing & Spam Protection	• Prohibit Installation Without Privileged Status • Malicious Code Protection (Anti-Malware) • Integration of Detection & Response • Phishing & Spam Protection	• Endpoint Security • Endpoint Protection Measures • Prohibit Installation Without Privileged Status • Unauthorized Installation Alerts • Malicious Code Protection (Anti-Malware) • Automatic Updates • Documented Protection Measures • Centralized Management • Software Firewall • Integration of Detection & Response • Phishing & Spam Protection
Human Resources Security		• User Awareness • Terms of Employment • Personnel Termination	• Roles & Responsibilities • User Awareness • Personnel Screening • Terms of Employment • Rules of Behavior • Social Media & Social Networking Restrictions • Use of Communications Technology • Use of Mobile Devices • Confidentiality Agreements • Post-Employment Obligations • Personnel Sanctions • Personnel Termination • Asset Collection • High-Risk Terminations • Post-Employment Requirements • Identify Critical Skills & Gaps

			• Remediate Identified Skills Deficiencies
Identification & Authentication	• Multi-Factor Authentication (MFA) • Password Managers	• Multi-Factor Authentication (MFA) • User Provisioning & De-Provisioning • Automated Support For Password Strength • Vendor-Supplied Defaults • Password Managers • Least Privilege • Account Lockout	• Identity & Access Management (IAM) • Identification & Authentication for Non-Organizational Users • Identification & Authentication for Devices • Multi-Factor Authentication (MFA) • Network Access to Privileged Accounts • User Provisioning & De-Provisioning • Role-Based Access Control (RBAC) • Authenticator Management • Password-Based Authentication • Automated Support For Password Strength • Vendor-Supplied Defaults • Password Managers • Disable Inactive Accounts • Automated Audit Actions • Account Disabling for High Risk Individuals • System Accounts • Usage Conditions • Privileged Account Management (PAM) • Privileged Account Inventories • Periodic Review • User Responsibilities for Account Management • Credential Sharing • Access Enforcement • Least Privilege

			• Non-Privileged Access for Non-Security Functions • Prohibit Non-Privileged Users from Executing Privileged Functions • Account Lockout • Session Lock • Identity Evidence Validation & Verification
Incident Response		• Incident Response Plan (IRP) • Data Breach	• Incident Response Operations • Incident Handling • Indicators of Compromise (IOC) • Incident Response Plan (IRP) • Data Breach • Incident Response Training • Integrated Security Incident Response Team (ISIRT) • Situational Awareness For Incidents • Incident Stakeholder Reporting • Cyber Incident Reporting for Sensitive Data • Vulnerabilities Related To Incidents • Supply Chain Coordination • Coordination With External Providers • Regulatory & Law Enforcement Contacts • Public Relations & Reputation Repair
Information Assurance			• Assessments • Specialized Assessments • Third-Party Assessments
Maintenance			• Maintenance Operations • Maintenance Tools

			• Inspect Tools • Inspect Media • Restrict Tool Usage • Remote Maintenance
Mobile Device Management			• Centralized Management Of Mobile Devices • Full Device & Container-Based Encryption • Organization-Owned Mobile Devices
Network Security	• Network Intrusion Detection / Prevention Systems (NIDS / NIPS) • Sender Policy Framework (SPF) • DNS & Content Filtering	• Guest Networks • Network Intrusion Detection / Prevention Systems (NIDS / NIPS) • Sender Policy Framework (SPF) • Work From Anywhere (WFA) - Telecommuting Security • Data Loss Prevention (DLP) • DNS & Content Filtering	• Network Security Management • Layered Network Defenses • Guest Networks • Personal Data (PD) • Prevent Unauthorized Exfiltration • Dynamic Isolation & Segregation (Sandboxing) • Data Flow Enforcement – Access Control Lists (ACLs) • Deny Traffic by Default & Allow Traffic by Exception • Network Segmentation • Virtual Local Area Network (VLAN) Separation • Remote Session Termination • Network Intrusion Detection / Prevention Systems (NIDS / NIPS) • Sender Policy Framework (SPF) • Domain Registrar Security • End-User Messaging Technologies • Remote Access

			• Protection of Confidentiality / Integrity Using Encryption • Work From Anywhere (WFA) - Telecommuting Security • Disable Wireless Networking • Data Loss Prevention (DLP) • DNS & Content Filtering
Physical & Environmental Security			• Physical & Environmental Protections • Lockable Physical Casings • Physical Security of Offices, Rooms & Facilities • Intrusion Alarms / Surveillance Equipment • Emergency Lighting • Water Damage Protection • Fire Protection • Fire Detection Devices
Privacy	• Security of Personal Data	• Security of Personal Data • Personal Data Retention & Disposal	• Privacy Program • Chief Privacy Officer (CPO) • Data Protection Officer (DPO) • Security of Personal Data • Privacy Notice • Purpose Specification • Authority To Collect, Use, Maintain & Share Personal Data (PD) • Personal Data Retention & Disposal • Inventory of Personal Data (PD) • Information Sharing With Third Parties

Project & Resource Management			• Security Portfolio Management • Strategic Plan & Objectives • Allocation of Resources
Risk Management		• Risk Assessment	• Risk Management Program • Risk Assessment • Risk Register • Risk Response • Supply Chain Risk Assessment • Risk Monitoring
Secure Engineering & Architecture		• Defense-In-Depth (DiD) Architecture	• Secure Engineering Principles • Defense-In-Depth (DiD) Architecture • Technology Lifecycle Management • Fail Secure • System Use Notification (Logon Banner) • Standardized Microsoft Windows Banner
Security Operations		• Defense-In-Depth (DiD) Architecture	• Standardized Operating Procedures (SOP) • Security Operations Center (SOC) • Secure Practices Guidelines
Security Awareness & Training		• Security & Privacy-Minded Workforce	• Security & Privacy-Minded Workforce • Security & Privacy Awareness • Practical Exercises • Social Engineering & Mining • Role-Based Security & Privacy Training • Suspicious Communications & Anomalous System Behavior

			• Sensitive Information Storage, Handling & Processing • Privileged Users • Cyber Threat Environment • Security & Privacy Training Records
Technology Development & Acquisition		• Ports, Protocols & Services In Use • Unsupported Systems	• Ports, Protocols & Services In Use • Development Methods, Techniques & Processes • Documentation Requirements • Separation of Development, Testing and Operational Environments • Continuous Monitoring Plan • Developer Threat Analysis & Flaw Remediation • Unsupported Systems
Third-Party Management		• Third-Party Risk Assessments & Approvals	• Third-Party Management • Third-Party Inventories • Third-Party Criticality Assessments • Third-Party Services • Third-Party Risk Assessments & Approvals • Identification of Functions, Ports, Protocols & Services • Security Compromise Notification Agreements
Threat Management			• Threat Intelligence Program • Threat Intelligence Feeds • Insider Threat Program
Vulnerability & Patch Management		• Vulnerability Scanning	• Vulnerability & Patch Management Program (VPMP)

			• Vulnerability Remediation Process • Continuous Vulnerability Remediation Activities • Stable Versions • Software & Firmware Patching • Centralized Management • Automated Remediation Status • Automated Software & Firmware Updates • Vulnerability Scanning • Internal Vulnerability Assessment Scans • Penetration Testing
Web Security			• Web Security • Web Application Firewall (WAF) • Secure Web Traffic