

WISP Domain	WISP Standard Name	WISP Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials	
Security & Privacy Governance	Security & Privacy Governance Program	GOV-1	Identify				CC1.2		GRM-04	5.1.1	PM-1			12.1 12.1.1	§ 1232h	6801(b)(1)	164.306 164.306(a) 164.306(b) 164.306(c) 164.306(d) 164.306(e)	17.03(1) 17.04 17.03(2)(b)(2)	500.02		Sec 10		
Security & Privacy Governance	Publishing Security & Privacy Documentation	GOV-2	Identify	ID.GV-1			CC5.3		AIS-04 GRM-05 GRM-06	5.1.1	PM-1			12.1 12.1.1	§ 1232h	6801(b)(1)	164.306 164.308 164.308(a)(1)(i) 164.312 164.316 164.316(a)	17.03(1) 17.04 17.03(2)(b)(2)	500.03		Sec 10		
Security & Privacy Governance	Assigned Security & Privacy Responsibilities	GOV-3	Identify	ID.AM-6			CC1.1 CC1.3		GRM-05		PL-9 PM-2 PM-6			12.5-12.5.5		Safeguards Rule	164.308(a)(2)	17.03(2)(a)	500.04	622(2)(d)(A)(i)	Sec 9		
Security & Privacy Governance	Measures of Performance	GOV-4	Protect	PR.IP-8			CC1.2 CC1.5 CC2.2				PM-6									17.03(2)(j)	622(2)(d)(A)(vi) 622(2)(d)(B)(iii)	Sec 10 Sec 11	
Asset Management	Asset Governance	AST-1	Identify					1.4 1.5 2.6			PM-5			12.3.3 12.3.4 12.3.7									
Asset Management	Asset Inventories	AST-2	Identify	ID.AM-1 ID.AM-2 ID.AM-4		CM.2.061		1.4 1.5 1.6 2.1 2.5 16.1		8.1.1	CM-8 PM-5	3.4.1		1.1.2 2.2.4			164.310(d)(2)(iii)						
Asset Management	Network Diagrams & Data Flow Diagrams (DFDs)	AST-3	Identify	ID.AM-3			CC2.1	12.1 12.9	DSI-02 IVS-13		PL-2 SA-5(1) SA-5(2) SA-5(3) SA-5(4)			1.1.2 1.1.3									
Asset Management	Secure Disposal or Re-Use of Equipment	AST-4	Identify		52.204-21(b)(1)(vii)		CC6.5		DCS-05	11.2.7				9.8-9.8.2			164.310(d)(2)(i) 164.310(d)(2)(ii)						
Asset Management	Removal of Assets	AST-5	Protect	PR.DS-3					DCS-04	11.2.5							164.310(d)(1) 164.310(d)(2)			622(2)(d)(C)(ii)			
Business Continuity & Disaster Recovery	Business Continuity Management System (BCMS)	BCD-1	Recover	RC.RP-1		RE.5.140	CC7.5 CC9.1		BCR-01 BCR-07	17.1.2	CP-1 CP-2 IR-4(3) PM-8 CP-10						164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(b)						
Business Continuity & Disaster Recovery	Identify Critical Assets	BCD-2	Recover	ID.BE-05			CC7.5				CP-2(8)						164.308(a)(7)(ii)(E)						
Business Continuity & Disaster Recovery	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-3	Detect	RC.IM-1			CC7.5				CP-4												
Business Continuity & Disaster Recovery	Contingency Planning & Updates	BCD-4	Recover	RC.IM-2			CC7.5				CP-2												

WISP Domain	WISP Standard Name	WISP Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials	
Business Continuity & Disaster Recovery	Data Backups	BCD-5	Protect	PR.IP-4		RE.2.137 RE.3.139	CC7.5 A1.2	10.1 10.2 10.4		12.3.1	CP-9 SC-28(2)	3.8.9					164.308(a)(7)(H)(A) 164.310(d)(2)(iv)						
Business Continuity & Disaster Recovery	Testing for Reliability & Integrity	BCD-6	Recover				CC7.5 A1.2	10.3			CP-9(1)												
Business Continuity & Disaster Recovery	Information System Recovery & Reconstitution	BCD-7	Protect	PR.IP-4			CC7.5 A1.2	5.5 10.5			CP-10												
Capacity & Performance Planning	Capacity & Performance Management	CAP-1	Protect	PR.DS-4			A1.1		IVS-04	12.1.3	SC-5 SC-5(3)												
Capacity & Performance Planning	Resource Priority	CAP-2	Protect				A1.1				SC-5 SC-5(1) SC-5(2) SC-6												
Capacity & Performance Planning	Capacity Planning	CAP-3	Protect				A1.1				SC-5 SC-5(2) CP-2(2)												
Change Management	Change Management Program	CHG-1	Protect				CC3.4 CC8.1	5.5		12.1.2	CM-3												
Change Management	Configuration Change Control	CHG-2	Protect	PR.IP-3		CM.2.065	CC3.4 CC8.1	5.5	MOS-15	14.2.2	CM-3	3.4.3		6.4-6.4.6									
Cloud Security	Cloud Services	CLD-1	Protect		52.204-21(b)(1)(iv)									2.6 12.8.1									
Cloud Security	Cloud Security Architecture	CLD-2	Protect		52.204-21(b)(1)(iv)				STA-03														
Cloud Security	Security Management Subnet	CLD-3	Protect		52.204-21(b)(1)(iv)	SC.4.228		4.6 11.7				3.13.2											
Cloud Security	Application & Program Interface (API) Security	CLD-4	Protect		52.204-21(b)(1)(iv)				AIS-01 IPY-01														
Cloud Security	Multi-Tenant Environments	CLD-5	Protect		52.204-21(b)(1)(iv)				IVS-09														

WISP Domain	WISP Standard Name	WISP Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials
Cloud Security	Data Handling & Portability	CLD-6	Protect		52.204-21(b)(1)(iv)				IVS-10													
Cloud Security	Geolocation Requirements for Processing, Storage and Service Locations	CLD-7	Protect		52.204-21(b)(1)(iv)				DSA-02		SA-9(5)											
Cloud Security	Sensitive Data In Public Cloud Providers	CLD-8	Protect		52.204-21(b)(1)(iv)																	
Compliance	Statutory, Regulatory & Contractual Compliance	CPL-1	Identify	ID.GV-3 PR.IP-5 DE.DP-2	52.204-21(b)(2) 52.204-21(c)		CC2.2 CC2.3			18.1.1	PL-1 PM-8	NFO - PL-1		12.1		6801(b)(3)	164.302 164.318 164.318(a) 164.318(a)(1) 164.318(a)(2) 164.318(b)	500.19				
Compliance	Security Controls Oversight	CPL-2	Detect	DE.DP-5 PR.IP-7		CA.2.158 CA.3.161	CC2.2 CC2.3		AAC-02 AAC-03 GRM-03		CA-7 CA-7(1) PM-14	3.12.1 3.12.3		12.11 12.11.1			164.308(a)(8)		622(2)(B)(iii)	Sec 10 Sec 11		
Configuration Management	Configuration Management Program	CFG-1	Protect				CC7.1	5.5			CM-1 CM-9	NFO - CM-1 NFO - CM-9		1.1.5								2
Configuration Management	System Hardening Through Baseline Configurations	CFG-2	Protect	PR.IP-1 PR.IP-3		CM.2.064 SC.5.230	CC7.1 CC8.1	5.1 5.2 5.3 5.5 6.2 6.2 8.3	GRM-01 IVS-07	14.1.1	CM-2 CM-6 SA-8	3.4.2	A1 A2 A3 A4 A5 A6	1.1 1.1.1 2.2-2.2.4								2
Configuration Management	Least Functionality	CFG-3	Protect	PR.PT-3	52.204-21(b)(1)(ii)	CM.2.062		9.1 9.2 12.4	IAM-03		CM-7	3.4.6	A6	1.1.5 1.2.1 2.2.2 2.2.4 2.2.5				17.03(2)(a) 17.03(2)(g)				
Monitoring	Continuous Monitoring	MON-1	Detect	DE.CM-1 DE.DP-1 DE.DP-2 PR.PT-1			CC7.2	6.2 6.8	IAM-04 IVS-06	12.4.1	AU-1 SI-4	NFO - AU-1	A2 A5 A10	10.1 10.6-10.6.3 10.8-10.8.1			164.312(b)	500.06				
Monitoring	File Integrity Monitoring (FIM)	MON-2	Detect	PR.DS-8			CC6.8 CC7.1	6.8					A3 A4 A5 AT A8 A10	11.5-11.5.1			164.312(c) 164.312(c)(1) 164.312(c)(2)					
Monitoring	Centralized Collection of Security Event Logs	MON-3	Detect			AU.3.048	CC7.2 CC7.3	6.2 6.4 6.5 6.6 6.8			AU-2 AU-2(3) AU-6 SI-4		A10	10.2.1-10.2.7 11.4				17.03(2)(b)(3) 17.04(4)		622(2)(d)(B)(iii)		
Monitoring	Monitoring Reporting	MON-4	Detect	DE.DP-4		AU.3.052	CC7.2 CC7.3	6.7			AU-7 AU-7(1) AU-12	3.3.6										
Monitoring	Anomalous Behavior	MON-5	Detect	DE.AE-1		SI.5.222 SI.5.223	CC7.2	16.8 16.13 20.8			AC-2(12) SI-4(11)			10.6-10.6.2								

WISP Domain	WISP Standard Name	WISP Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials
Monitoring	Insider Threats	MON-6	Detect	DE.CM-3																		
Monitoring	Third-Party Threats	MON-7	Detect	DE.CM-6																		
Monitoring	Unauthorized Activities	MON-8	Detect	DE.CM-7																		
Cryptographic Protections	Use of Cryptographic Controls	CRY-1	Protect			SC.3.177	CC6.1	1.8 14.4 14.8 15.7 15.8 18.5	EKM-03 EKM-04	10.1.1	SC-8(2) SC-13 SC-13(1) SI-7(6)	3.13.11		2.2.3 4.1			164.312(a)(2)(iv)	500.15				
Cryptographic Protections	Transmission Confidentiality	CRY-2	Protect	PR.DS-2		SC.2.179	CC6.1 CC6.7	11.5 12.11 14.4 16.5	IVS-10	13.2.3	SC-8						164.312(a)(2)(iv) 164.312(e) 164.312(e)(1) 164.312(e)(2)(ii)	17.04(3)	500.15	622(2)(d)(C)(iii)		
Cryptographic Protections	Transmission Integrity	CRY-3	Protect	PR.DS-8						14.1.3	SC-8 SC-16(1) SC-28(1)			3.4 3.4.1 4.1 9.8.2			164.312(c) 164.312(c)(1) 164.312(c)(2) 164.312(e)(2)(i)	17.04(3)		622(2)(d)(C)(iii)		
Cryptographic Protections	Encrypting Data At Rest	CRY-4	Protect	PR.DS-1		MP.3.125	CC6.1 CC6.7	13.9 14.8		10.1.1	SC-13 SC-28(2)	3.8.6		3.4 3.4.1			164.312(a)(2)(iv)	17.04(5)	500.15	622(2)(d)(C)(iii)		
Data Classification & Handling	Data Protection	DCH-1	Protect			MP.2.119	CC2.1 CC6.7 C1.1 PI1.5	13.1 14.4 14.8		8.2 8.3.3	MP-1	3.8.1 NFO - MP-1		9.7-9.7.1	§ 1232g § 1232h				17.03(2)(c)		Sec 13	
Data Classification & Handling	Data & Asset Classification	DCH-2	Identify	ID.AM-5			CC2.1 C1.1	13.1	DSI-01 DCS-01	8.2.1				9.6.1								
Data Classification & Handling	Media Access	DCH-3	Protect		52.204-21(b)(1)(vii)	MP.2.120	C1.1				MP-2	3.8.2			§ 1232h							
Data Classification & Handling	Media Storage	DCH-4	Protect		52.204-21(b)(1)(vii)						MP-4			9.5 9.5.1 9.6-9.6.2 9.7.9.				17.03(2)(c)		622(2)(d)(C)(i) 620		
Data Classification & Handling	Physical Media Disposal	DCH-5	Protect	PR.IP-6	52.204-21(b)(1)(vii)		CC6.5		DSI-07	8.3.2	MP-6											
Data Classification & Handling	Digital Media Sanitization	DCH-6	Protect	PR.IP-6	52.204-21(b)(1)(vii)	MA.3.115 MP.1.118	CC6.5				MP-6 MP-6(3)	3.7.3 3.8.3		9.8-9.8.2						622(2)(d)(C)(i) 622(2)(d)(C)(iv)		

WISP Domain	WISP Standard Name	WISP Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials
Data Classification & Handling	Removable Media Security	DCH-7	Protect	PR.PT-2			CC6.7	13.7 13.8 13.9		8.3.1												
Data Classification & Handling	Use of External Information Systems	DCH-8	Protect		52.204-21(b)(1)(iii)	AC.1.003	CC6.7		AIS-02		AC-20	3.1.20										
Data Classification & Handling	Limits of Authorized Use	DCH-9	Protect		52.204-21(b)(1)(iii)						AC-20(1)											
Data Classification & Handling	Portable Storage Devices	DCH-10	Protect		52.204-21(b)(1)(iii)	AC.2.006	CC6.7				AC-20(2)	3.1.21										
Data Classification & Handling	Protecting Sensitive Data on External Systems	DCH-11	Protect		52.204-21(b)(1)(iii)																	
Data Classification & Handling	Publicly Accessible Content	DCH-12	Protect		52.204-21(b)(1)(iv)	AC.1.004					AC-22	3.1.22										
Data Classification & Handling	Data Mining Protection	DCH-13	Protect		52.204-21(b)(1)(iv)						AC-23											
Data Classification & Handling	Ad-Hoc Transfers	DCH-14	Protect		52.204-21(b)(1)(iii)		CC6.7															
Data Classification & Handling	Media & Data Retention	DCH-15	Protect				PI1.5	14.6	BCR-11	8.3 18.1.3	MP-7 SI-12			3.1 3.2-3.2.3 10.7			164.316(b)(2) 164.316(b)(2)(f) 164.530(j)(1)	500.12	622(2)(C)(i) (iv)			
Data Classification & Handling	Information Disposal	DCH-16	Protect		52.204-21(b)(1)(vii)		CC6.5 CI.2 P4.3				DM-2											
Endpoint Security	Endpoint Security	END-1	Protect						HRS-11	11.2.9	MP-2						164.310(c)					4
Endpoint Security	Malicious Code Protection (Anti-Malware)	END-2	Detect	DE.CM-4	52.204-21(b)(1)(xii) 52.204-21(b)(1)(xiii) 52.204-21(b)(1)(xiv) 52.204-21(b)(1)(xv)	SI.1.211	CC6.8	8.1 8.4 8.5 8.6	TVM-01	12.2.1	SI-3	3.14.2		5.1-5.1.2 5.2 5.3				17.04(7)				4
Endpoint Security	Automatic Updates	END-3	Protect		52.204-21(b)(1)(xiv)	SI.1.212		8.2			SI-3(2)	3.14.4		5.2								4

WISP Domain	WISP Standard Name	WISP Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials	
Endpoint Security	Always On Protection	END-4	Detect		52.204-21(b)(1)(xv)	SI.1.213						3.14.5		5.3									
Endpoint Security	File Integrity Monitoring (FIM)	END-5	Protect	PR.DS-6			CC6.8	14.9			SI-7			11.5-11.5.1									
Endpoint Security	Mobile Code	END-6	Detect	DE.CM-5		SC.3.188			TVM-03		SC-18 SC-18(1) SC-18(2) SC-18(3) SC-18(4) SC-27	3.13.13											
Human Resources Security	Human Resources Security Management	HRS-1	Protect	PR.IP-11			CC1.1 CC1.4 CC1.5				PS-1	NFO - PS-1											
Human Resources Security	Roles & Responsibilities	HRS-2	Identify	DE.DP-1			CC1.2 CC1.3 CC2.2		HRS-04 HRS-07	6.1.1 7.2	PM-13			12.4 12.4.1			164.308(a)(2)						
Human Resources Security	Terms of Employment	HRS-3	Identify				CC1.1		HRS-03	7.1.2 7.2.1													
Human Resources Security	Rules of Behavior	HRS-4	Identify		52.204-21(b)(1)(iv)		CC1.1		HRS-08 MOS-06	7.2.1 8.1.3	PL-4	NFO - PL-4		4.2 12.3-12.3.2 12.3.5-6 12.3.10 12.4			164.310(b)	17.03(2)(b)(2)					
Human Resources Security	Social Media & Social Networking Restrictions	HRS-5	Identify		52.204-21(b)(1)(iv)	SC.3.193					PL-4(1)	NFO - PL-4(1)											
Identification & Authentication	Identity & Access Management (IAM)	IAC-1	Protect		52.204-21(b)(1)(i)		CC6.1	4.4 16.1 16.2 16.6 16.7 16.10	IAM-01 IAM-02 IAM-04 IAM-08 IAM-12	9.1.1	AC-1 IA-1	NFO - AC-1 NFO - IA-1	A2 A5	8.1.8.4			164.308(a)(4)(i) 164.308(a)(4)(ii)(A) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a) 164.312(a)(1)	500.07				2	
Identification & Authentication	Identification & Authentication for Organizational Users	IAC-2	Protect		52.204-21(b)(1)(i) 52.204-21(b)(1)(v) 52.204-21(b)(1)(vi)	IA.1.076 IA.1.077	CC6.1	16.10 16.13	IAM-09		IA-2	3.5.1 3.5.2		8.1.1.8.2			164.312(a)(2)(i)						2
Identification & Authentication	Identification & Authentication for Devices	IAC-3	Protect		52.204-21(b)(1)(v)		CC6.1	16.6	DCS-03		IA-3 IA-3(1) IA-3(4)												
Identification & Authentication	Multi-Factor Authentication (MFA)	IAC-4	Protect	PR.AC-7		IA.3.083		1.8 4.5 11.5 12.11 16.3		11.1.2	IA-2(11)	3.5.3	A2	8.3-8.3.2					500.12				2
Identification & Authentication	User Provisioning & De-Provisioning	IAC-5	Protect	PR.AC-6			CC6.2	16.7	IAM-09 IAM-11 IAM-09 IAM-11	9.2.1 9.2.2	IA-5(3)		A5				164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B)						3

WISP Domain	WISP Standard Name	WISP Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials
Identification & Authentication	Role-Based Access Control (RBAC)	IAC-6	Protect		52.204-21(b)(1)(i) 52.204-21(b)(1)(ii)		CC6.1 CC6.3	14.6	IAM-04		AC-2(7)		A5	7.1-7.1.4 7.2-7.2.3			164.308(a)(3)(i)					3
Identification & Authentication	Authenticator Management (Passwords)	IAC-7	Protect		52.204-21(b)(1)(v) 52.204-21(b)(1)(vi)	IA.2.079 IA.2.080	CC6.1	4.4 16.4		9.2.3 9.2.4 9.4.3	IA-5 IA-5(4)	3.5.8 3.5.9		8.1.2 8.2-8.2.6				17.04(1)(b)-(e) 17.04(2)(b)				2
Identification & Authentication	Account Management	IAC-8	Protect	PR.AC-1	52.204-21(b)(1)(i) 52.204-21(b)(1)(ii)	AC.1.002	CC6.1	16.13	IAM-10		AC-2	3.1.2		8.1.3-8.1.5 8.2.2 8.5-8.5.1 8.6 8.7			164.312(a)(2)(ii)	17.04(1)(a)				
Identification & Authentication	Access Enforcement	IAC-9	Protect		52.204-21(b)(1)(i) 52.204-21(b)(1)(ii)	AC.1.001	CC6.1			9.2.6 9.4	AC-3 AC-6	3.1.1	A5	7.1-7.1.4 7.2-7.2.1 7.2.3				17.04(1)(b) 17.04(2)(a)	622(2)(d)(C)(iii)			
Identification & Authentication	Least Privilege	IAC-10	Protect	PR.AC-4	52.204-21(b)(1)(i)	AC.2.007	CC6.1	14.6		9.1.2	AC-6	3.1.5	A5						622(2)(d)(C)(iii)			
Incident Response	Incident Response Operations	IRO-1	Protect	PR.IP-9			CC7.3 CC7.4			16.1.1	IR-1	NFO - IR-1					164.308(a)(6) 164.308(a)(6)(i) 164.308(a)(6)(ii)	500.16			Sec 8	
Incident Response	Incident Handling	IRO-2	Respond	DE.AE-2 DE.AE-4 DE.AE-5 RS.AN-1 RS.AN-4 RS.MI-1		IR.2.092 IR.2.094 IR.2.095 IR.3.098 IR.4.100 RM.4.149	CC7.3 CC7.4			16.1.4	IR-4	3.6.1 3.6.2		12.5.3 12.10							Sec 8	
Incident Response	Indicators of Compromise (IOC)	IRO-3	Respond	RS.AN-2																		
Incident Response	Incident Response Plan (IRP)	IRO-4	Respond	RS.RP-1			CC7.3 CC7.4	19.1 19.2 19.3 19.8	SEF-02	16.1.5	IR-8	NFO - IR-8		12.8.3 12.10-12.10.6					500.16	622(2)(d)(B)(iii)		
Incident Response	IRP Update	IRO-5	Respond	RS.IM-2							IR-1	NFO - IR-1										
Incident Response	Incident Response Testing	IRO-6	Respond			IR.3.099 IR.5.110					IR-3 SI-4(9)	3.6.3		12.10.2								
Incident Response	Coordination with Related Plans	IRO-7	Protect	PR.IP-10							IR-3(2)											
Incident Response	Integrated Security Incident Response Team (ISIRT)	IRO-8	Respond	RC.CO-1 RC.CO-2 RC.CO-3 RS.CO-1 RS.CO-4		IR.5.108	CC7.4	19.3		16.1.4	IR-10			12.10.3							Sec 8 Sec 9	

WISF Domain	WISF Standard Name	WISF Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials	
Incident Response	Chain of Custody & Forensics	IRO-9	Respond	RS.AN-3		IR.5.106			SEF-04	16.1.7	AU-10(3)												
Incident Response	Situational Awareness For Incidents	IRO-10	Detect	DE.AE-3		IR.2.093	CC7.4		SEF-05		IR-5			12.5.2 12.10.5									
Incident Response	Incident Stakeholder Reporting	IRO-11	Respond	RS.CO-2 RS.CO-3 RS.CO-5	52.204-21(b)(1)(xii)		CC2.3 CC7.4 P6.3 P6.7	19.4 19.6		16.1.2 16.1.3	IR-6			12.5.2 12.8.3			164.314(a)(2)(i)(C) 164.404 164.404(a) 164.404(a)(1) 164.404(a)(2) 164.404(b)	17.03(2)(j)	500.17	604(1)-(5)	Sec 8		
Incident Response	Root Cause Analysis (RCA) & Lessons Learned	IRO-12	Respond	RS.IM-1		IR.2.097				16.1.6	IR-1	NFO - IR-1		12.10.6									
Maintenance	Maintenance Operations	MNT-1	Protect							11.2.4	MA-1	NFO - MA-1	A9				164.310(a)(2)(iv)						
Maintenance	Controlled Maintenance	MNT-2	Protect	PR.MA-1		MA.2.111					MA-2	3.7.1	A9				164.310(a)(2)(iv)						
Maintenance	Non-Local Maintenance	MNT-3	Protect	PR.MA-2		MA.2.113					MA-4	3.7.5											
Network Security	Network Security Management	NET-1	Protect	PR.PT-4			CC6.1 CC6.6	11.1 11.2	IPY-04	13.1.1 13.1.2	SC-1	NFO - SC-1										1	
Network Security	Layered Network Defenses	NET-2	Protect	PR.AC-5		SC.5.208	CC6.6	9.5						1.3.7									
Network Security	Guest Networks	NET-3	Protect		52.204-21(b)(1)(xi)			15.10						1.2.3									
Network Security	Boundary Protection	NET-4	Protect		52.204-21(b)(1)(x) 52.204-21(b)(1)(xi)	SC.1.175 SC.4.197	CC6.1 CC6.6 CC6.8	9.5 12.8 12.9			SC-7 SC-7(9) SC-7(11)	3.13.1		1.1.3 1.1.4 1.2.1 1.2.3 1.3								1	
Network Security	Isolation of Information System Components (DMZ)	NET-5	Protect		52.204-21(b)(1)(xi)						SC-7(21)												
Network Security	Data Flow Enforcement – Access Control Lists (ACLs)	NET-6	Protect			AC.2.016 AC.4.023	CC6.1 CC6.6	11.2		9.4.1 13.1.1 14.1.2	AC-4	3.1.3		1.1-1.1.7 1.2-1.2.3 1.3.3 1.3.5 7.2-7.2.3						622(2)(d)(C)(iii)			

WISP Domain	WISP Standard Name	WISP Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials	
Network Security	External System Connections	NET-7	Protect		52.204-21(b)(1)(iii)		CC6.1				CA-3(3)			1.3 1.3.3 1.3.5									
Network Security	Network Segmentation	NET-8	Protect		52.204-21(b)(1)(xi)	SC.1.176	CC6.1	11.7 14.1 14.2 14.3			AC-4(21)	3.13.5											
Network Security	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-9	Protect				CC6.8	12.3 12.4 12.6 12.7						11.4									
Network Security	DMZ Networks	NET-10	Protect		52.204-21(b)(1)(xi)		CC6.6																
Network Security	Remote Access	NET-11	Protect	PR.AC-3	52.204-21(b)(1)(i) 52.204-21(b)(1)(ii)		CC6.6	12.12		6.2.2	AC-17 AC-17(6)			12.3.8 12.3.9									
Physical & Environmental Security	Physical & Environmental Protections	PES-1	Protect			PE.2.135	CC6.4 A1.2			11.1.4 18.1.4	PE-1	3.10.2 NFO - PE-1					164.310 164.310(a) 164.310(a)(1) 164.310(a)(2)(ii)						
Physical & Environmental Security	Physical Access Authorizations	PES-2	Protect		52.204-21(b)(1)(viii)	PE.1.131	CC6.4			11.1.1	PE-2	3.10.1		9.2			164.310(a)(2)(ii) 164.310(a)(2)(iii)						
Physical & Environmental Security	Physical Access Control	PES-3	Protect	PR.AC-2	52.204-21(b)(1)(k)	PE.1.134	CC6.4		DCS-02	9.1.1	PE-3 PE-3(2) PE-3(3)	3.10.5		9.1-9.1.2 9.2 9.4.2 9.4.3				17.03(2)(g)		622(2)(d)(C)(ii)			
Physical & Environmental Security	Controlled Ingress & Egress Points	PES-4	Protect		52.204-21(b)(1)(k)				DCS-07 DCS-08					9.1-9.1.3									
Physical & Environmental Security	Physical Access Logs	PES-5	Protect		52.204-21(b)(1)(k)	PE.1.133					PE-8	3.10.4 NFO - PE-8		9.4.4							622(2)(d)(C)(ii)		
Physical & Environmental Security	Physical Security of Offices, Rooms & Facilities	PES-6	Protect						DCS-06	11.1.1 11.1.3 11.2.9				9.3									
Physical & Environmental Security	Working in Secure Areas	PES-7	Protect							11.1.2 11.1.5													
Physical & Environmental Security	Monitoring Physical Access	PES-8	Detect	DE.CM-2	52.204-21(b)(1)(viii) 52.204-21(b)(1)(k)						PE-6			9.1-9.1.1							622(2)(d)(C)(ii)		

WISP Domain	WISP Standard Name	WISP Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials	
Physical & Environmental Security	Visitor Control	PES-9	Protect		52.204-21(b)(1)(k)	PE.1.132						3.10.3		9.4-9.4.4									
Physical & Environmental Security	Distinguish Visitors from On-Site Personnel	PES-10	Protect		52.204-21(b)(1)(k)									9.2									
Physical & Environmental Security	Identification Requirement	PES-11	Protect								PE-2(2)			9.4-9.4.3						622(2)(d)(C)(ii)			
Physical & Environmental Security	Restrict Unescorted Access	PES-12	Protect		52.204-21(b)(1)(k)	PE.1.132					PE-2(3)	3.10.3		9.3									
Physical & Environmental Security	Equipment Siting & Protection	PES-13	Protect				A1.2		BCR-06	11.1.4 11.2.1 11.2.3	PE-18 PE-18(1) SC-7(14)												
Physical & Environmental Security	Access Control for Transmission Medium	PES-14	Protect							11.2.3	PE-4 SC-7(14)			9.1.2 9.1.3						622(2)(d)(C)(ii)			
Physical & Environmental Security	Access Control for Output Devices	PES-15	Protect		52.204-21(b)(1)(viii)		PI1.4				PE-5									622(2)(d)(C)(ii)			
Physical & Environmental Security	Information Leakage Due To Electromagnetic Signals Emanations	PES-16	Protect	PR.D5-5			A1.2				PE-19												
Project & Resource Management	Security Portfolio Management	PRM-1	Identify				CC3.1 CC5.2			6.1.5	PL-1	NFO - PL-1										Sec 12	
Project & Resource Management	Allocation of Resources	PRM-2	Identify	ID.BE-3			CC3.1				SA-2	NFO - SA-2										Sec 12	
Project & Resource Management	Security & Privacy In Project Management	PRM-3	Identify				CC3.1 CC5.2			6.1.5	CA-2							17.03(2)(h)		622(2)(B)(i)-(iv)		Sec 12	
Project & Resource Management	Security & Privacy Requirements Definition	PRM-4	Identify	ID.BE-4 ID.BE-5			CC2.2 CC5.2			14.1	SA-14											Sec 12	
Project & Resource Management	Secure Development Life Cycle (SDLC) Management	PRM-5	Protect	PR.JP-2			CC5.2 CC8.1			14.2.2	SA-3	NFO - SA-3										Sec 12	

WISP Domain	WISP Standard Name	WISP Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials
Risk Management	Risk Management Program	RSK-1	Identify	ID.GV-4 ID.RM-1 ID.RM-2 ID.RM-3			CC3.1 CC5.1			11.1.4	PM-9 RA-1	NFO - RA-1		12.2		6801(b)(2)		17.03(2)(b)	500.09	622(2)(d)(A)(ii)	Sec 7	
Risk Management	Risk-Based Security Categorization	RSK-2	Identify				CC3.2				RA-2			9.6.1								
Risk Management	Risk Identification	RSK-3	Identify	ID.RA-3			CC3.2 CC7.2 A1.2														Sec 7	
Risk Management	Risk Assessment	RSK-4	Identify	ID.RA-5		RM.2.141 RM.3.144	CC3.2 CC7.3 A1.2	19.8	BCR-05 GRM-02 GRM-10	11.1.4	RA-3	3.11.1		12.2		Safeguards Rule	164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(D)	17.03(2)(b)		622(b)(A)(ii)	Sec 7 Sec 11	
Risk Management	Risk Ranking	RSK-5	Identify				CC3.2	3.7 19.8						6.1								
Risk Management	Risk Remediation	RSK-6	Identify	ID.RA-6		RM.2.143	CC3.2 CC4.2 CC7.4		GRM-11			3.11.3										
Risk Management	Business Impact Analysis (BIA)	RSK-7	Identify	ID.RA-4			CC3.2 CC5.2 PI1.1		BCR-08 BCR-09													
Risk Management	Supply Chain Risk Management Plan	RSK-8	Identify			RM.4.148	CC3.1 CC3.2				SA-12											
Secure Engineering & Architecture	Secure Engineering Principles	SEA-1	Protect	PR.JP-1 PR.PT-5	52.204-21(b)(1)(x) 52.204-21(b)(2)	SC.3.180	CC2.2 CC3.2 CC5.1 CC5.2		AIS-01 IPY-04	14.2.5	AR-7 SA-8 SA-13 SC-1 SC-7(18) SI-1	3.13.2	A5 A6	2.2			164.306(b) 164.306(c) 164.306(d) 164.308(a) 164.312 164.314(b)					
Secure Engineering & Architecture	Alignment With Enterprise Architecture	SEA-2	Protect				CC3.1 CC5.1			14.1.1	PL-8 PM-7	NFO - PL-8		2.2								
Secure Engineering & Architecture	Standardized Terminology	SEA-3	Protect		52.204-21(a)		CC2.2										164.304					
Secure Engineering & Architecture	Predictable Failure Analysis	SEA-4	Protect								SI-13									622(2)(d)(C)(iii)		
Secure Engineering & Architecture	Technology Lifecycle Management	SEA-5	Protect								SA-3	NFO - SA-3										

WISP Domain	WISP Standard Name	WISP Stanard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials	
Secure Engineering & Architecture	Fail Secure	SEA-6	Protect	PR.PT-5							CP-12 SC-24		A5 A6										
Security Awareness & Training	Security & Privacy-Minded Workforce	SAT-1	Protect	PR.AT-1 PR.AT-3 PR.AT-4			CC1.4	17.2 17.3 17.4 17.5 17.6 17.7	HRS-09	7.2.2	AT-1 PM-13	NFO - AT-1					164.308(a)(5) 164.308(a)(5)(i) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(5)(ii)(D)	500.14		Sec 6			
Security Awareness & Training	Security & Privacy Awareness	SAT-2	Protect			AT.2.056		17.3 17.9	MOS-01	7.2.2	AT-2	3.2.1		12.6				17.04(8) 17.03(2)(b)(1)					
Security Awareness & Training	Role-Based Security & Privacy Training	SAT-3	Protect	PR.AT-2 PR.AT-5		AT.2.057		17.2 17.9			AT-3	3.2.2		12.6.1			164.530(b) 164.530(b)(1) 164.530(b)(2)	17.04(8)		622(2)(d)(A)(iv)			
Security Awareness & Training	Privileged Users	SAT-4	Protect	PR.AT-2 PR.AT-5				18.6															
Security Awareness & Training	Security & Privacy Training Records	SAT-5	Protect								AT-4	NFO - AT-4		12.6.2									
Technology Development & Acquisition	Technology Development & Acquisition	TDA-1	Protect				CC5.2				PL-1 SA-1		A1 A2 A3 A4 A5 A6										
Technology Development & Acquisition	Separation of Development, Testing and Operational Environments	TDA-2	Protect	PR.DS-7					IVS-08	12.1.4	CM-4(1)			6.4.1									
Third-Party Management	Third-Party Management	TPM-1	Identify	ID.SC-1	52.204-21(c)		CC3.3 CC9.1		IAM-07 STA-05 STA-09	15.1.1	SA-4	NFO - SA-4	A3 A4	12.8			164.308(b) 164.308(b)(1) 164.308(b)(2)	500.11					
Third-Party Management	Third-Party Criticality Assessments	TPM-2	Identify	ID.BE-1 ID.SC-2			CC9.1				SA-14												
Third-Party Management	Supply Chain Protection	TPM-3	Identify	ID.SC-4			CC9.1		STA-01 STA-06	15.1.3	SA-12		A3 A4										
Third-Party Management	Third-Party Services	TPM-4	Identify				CC3.3			14.2.7 15.1.1	SA-9	NFO - SA-9	A3 A4	12.8.2 12.8.4				17.03(2)(f)(1)		622(2)(d)(A)(v)			
Third-Party Management	Third-Party Contract Requirements	TPM-5	Identify	ID.SC-3	52.204-21(c)		CC9.1			13.2.4 15.1.2	SA-9(3)			2.6 12.9			164.308(b)(3) 164.314 164.314(a) 164.314(a)(1) 164.314(a)(2) 164.314(a)(2)(iii)(A)						

WISP Domain	WISP Standard Name	WISP Standard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials
Third-Party Management	Third-Party Personnel Security	TPM-6	Identify	ID.GV-2			CC9.1															
Third-Party Management	Third-Party Incident Response & Recovery Capabilities	TPM-7	Identify	ID.SC-5			CC7.3 P6.5 P6.6															
Threat Management	Threat Intelligence Program	THR-1	Identify	ID.BE-2		RM.4.150 SA.4.171	CC3.3				PM-16			12.6					500.10			
Threat Management	Indicators of Exposure (IOE)	THR-2	Identify				CC3.3															
Threat Management	Threat Intelligence Feeds	THR-3	Identify	ID.RA-2 RS.AN-5	52.204-21(b)(1)(xii) 52.204-21(b)(1)(xiii)	SA.3.169					SI-5 SI-5(1)			6.2 12.4						622(2)(d)(B)(iii)		
Vulnerability & Patch Management	Vulnerability & Patch Management Program (VPMP)	VPM-1	Protect	ID.RA-1 PR.IP-12		SI.1.210			TVM-02	12.6.1	SI-2 SI-3(2)	3.14.1	A6 A9									5
Vulnerability & Patch Management	Vulnerability Remediation Process	VPM-2	Protect		52.204-21(b)(1)(xii)		CC4.2				PM-4 SC-18(1)		A6 A9					17.03(2)(j)		622(2)(d)(A)(i)		5
Vulnerability & Patch Management	Continuous Vulnerability Remediation Activities	VPM-3	Protect	RS.MI-3	52.204-21(b)(1)(xii)		CC4.2				SC-18(1)		A6 A9	6.6								
Vulnerability & Patch Management	Software Patching	VPM-4	Protect		52.204-21(b)(1)(xii) 52.204-21(b)(1)(xiii)			3.7		12.6.1	SI-2 SI-3(2)		A9	6.1 6.2				17.04(6)		622(2)(d)(B)(iii)		5
Vulnerability & Patch Management	Vulnerability Scanning	VPM-5	Detect	DE.CM-8		RM.2.142 RM.4.151	CC7.1	3.1 3.2 9.3 12.2	IVS-05		RA-5	3.11.2	A6 A9	11.2					500.05	622(2)(B)(iii) 622(2)(d)(A)(iii)		
Vulnerability & Patch Management	Red Team Exercises	VPM-6	Detect	DE.DP-3		CA.4.227		20.3 20.5 20.7			CA-8(2)											
Web Security	Web Security	WEB-1	Protect		52.204-21(b)(1)(iv)					13.1.3				1.3.1 1.3.2 1.3.4								
Web Security	Use of Demilitarized Zones (DMZ)	WEB-2	Protect		52.204-21(b)(1)(vi)					13.1.3				1.3.1 1.3.2 1.3.4								

WISP Domain	WISP Standard Name	WISP Stanard #	Function Grouping	NIST CSF v1.1	FAR 52.204-21	CMMC v1.02	AICPA TSC 2017 (SOC 2)	CIS CSC v7.1	CSA CCM v3.0.1	ISO 27002 v2013	NIST 800-53 rev4	NIST 800-171 rev 2	OWASP Top 10 v2017	PCI DSS v3.2	US FERPA	US GLBA	US HIPAA	US - MA 201 CMR 17.00	US - NY DFS 23 NYCRR500	US - OR 646A	US-TX Cybersecurity Act	EMEA UK Cyber Essentials	
Web Security	Client-Facing Web Services	WEB-3	Protect		52.204-21(b)(1)(iv)																		