Exhibit A: SHSP and UASI Allowable Cybersecurity Resource Expenditures by POETE Element

Table 1 provides examples of the types of resources that are allowable and encouraged under SHSP and UASI. The resource examples are not meant to be exhaustive and are provided only for consideration.

Table 1. Examples of resources (organized by POETE element) that can be funded through SHSP or UASI

POETE Element	Resource	Examples
Planning	Requirements and standards	Cybersecurity capability assessments
	Current cybersecurity and related response plans	• Cybersecurity Strategy • IT Security Plan • Cybersecurity Incident Response Plan • IT Disaster Recovery Plan
	Risk/configuration assessments	Penetration testing, contracted risk assessors
Organization	Internal personnel	Full time employees such as CISO, ISSO, network administrators, cybersecurity analysts, etc.
	External personnel	Contracted support such as cybersecurity service contractors, etc.
Equipment[1]	Software	Software such as anti-virus, anti-malware, continuous monitoring, encryption, enhanced remote authentication, patch management, distributed denial of service protection, etc.
	Hardware	Hardware such as intrusion detection systems, intrusion prevention systems (firewalls), additional servers, routers/switches, etc.
	Physical protection	Items such as fencing, cameras, locks (including electronic), biometrics readers, etc., to protect access to hardware and systems.
Training	Awareness-level training	Internal or external design, conduct, and evaluation of awareness-level training.
	Cybersecurity professional training	Internal or external design, conduct, and evaluation of professional-level cybersecurity training.
Exercise	Awareness drills	Drill preparation, conduct, and evaluation.
	Response/recovery exercises	Exercise preparation, conduct, and evaluation.

[1] Additional information on specific, pre-approved equipment can be found in the Authorized Equipment List (https://www.fema.gov/authorized-equipment-list).

Exhibit B: Example Cybersecurity Activities by NIST Function, POETE Element, and Outputs

Table 2 provides examples of allowable activities. They are organized by NIST function and POETE element and provide insight into the likely outputs from each activity. This is not an exhaustive list of activities that can be funded through HSGP, but rather strategic guidance to use as a framework in developing a cyber-focused investment justification.

Table 2. Activities, aligned to NIST function and POETE element, and their expected outcomes

NIST Function	Cybersecurity Activity	P	O	E	T	E	Measuring Progress of Outputs • Activity checklist items • Quarterly reports
Identify	Assess cybersecurity risks and threats.	✓					Yearly risk assessments.
	Develop an inventory of networks, devices, data, and systems.	✓					Inventory of networks, deployed hardware, data, and installed software.
	Establish governance structures for steady-state and response operations.	✓	✓				• CIO/CISO integrated in Senior Advisory Committee or Urban Area WG. • Documented information security policy, including legal and regulatory requirements. • Documented roles and responsibilities (e.g., CISO, CIO, CTO).
Protect	Develop mechanisms to manage access to networks, devices, and systems.		✓	✓			Centralized identity and privilege management, such as single sign-on, multi-factor authentication, and disabling/deleting accounts.
	Conduct awareness-level training for end-users.				✓		Awareness training campaigns, such as phishing and insider threat.
	Create and maintain a baseline configuration solution with appropriate security principles.	✓		✓			• Logs centralized, correlated, and consolidated • Logs synchronized with security information and event management (SIEM) software • Incorporated whitelisting
	Implement and test protection processes and procedures.	✓		✓		✓	Protective processes such as network segmentation (e.g., business side from infrastructure networks), privileged access, endpoint protection, public key infrastructure, and key management.
Detect	Set up technology and processes to monitor networks, devices, and system security.	✓		✓			Monitoring processes such as log management, configuration management, whitelisting, patching, and vulnerability management.
	Develop and test technology and processes to detect anomalies and events.			✓		✓	Security Operations Center (performing continuous monitoring functions).
	Set up procedures and organization to communicate anomaly and event detection.	✓	✓	✓			• Intrusion detection systems • Security information and event management solutions

NIST Function	Cybersecurity Activity	P	O	E	T	E	Measuring Progress of Outputs • Activity checklist items • Quarterly reports
Respond	Develop incident response and business continuity plans that incorporate lessons learned.	✓					Current response (including mitigation) and COOP plans.
	Set up procedures and organization to coordinate and communicate mitigation processes to all stakeholders.	✓	✓				Security Operations Center (performing response and mitigation functions).
Recovery	Develop incident recovery and disaster recovery plans that incorporate lessons learned.	✓					• Current recovery plans that incorporate lessons learned • Security Operations Center (performing recovery functions)
	Set up processes by which restoration is coordinated and communicated to all stakeholders.	✓	✓				Data Security