AELCode	Title	Description	Grant Notes
03OE-03-MEGA	System, Public Address, Handheld or Mobile	Systems for mass audio notification, including vehicle-mounted high powered speaker systems, or battery powered megaphone / public address systems with corded microphone.	
04AI-00-AI	Applications, Artificial Intelligence	Applications, systems, and services utilizing artificial intelligence design and algorithms to support enhanced threat and security capability,decision making and modeling, operational optimization, or task automation. May be implemented on local hardware, internet-based, or a hybrid. May also be provided as Software As A Service (SAAS, see 04AP-11-SAAS).	
04AP-05-CRED	System, Credentialing	Software application and associated hardware and material for creating site/event credential badges and controlling scene access. Although some hardware would still be required, this functionality may also be obtainable via subscription as a cloud-based service, as opposed to purchasing software. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information.	
04AP-06-VIDA	Software, Video Analytics	Software, either local or cloud-based, that analyzes video input to detect/determine temporal and spacial events, either in real time or using archival video. Analytical priorities might include recognition (e.g., facial or license plate recognition) or patterns (movement or arrangement or persons, vehicles, or other objects). See 04MD-01-VCAM and 13LE-00-SURV for examples of input devices.	For the Nonprofit Security Grant Program, license plate reader and facial recognition software are not allowed, but software to detect weapons through video analysis is allowed.
04AP-09-ALRT	Systems, Public Notification and Warning	Systems used to alert the public of protective actions or to provide warning to the public in the event of an incident, such as sirens, the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), and the Integrated Public Alert and Warning System (IPAWS).	Fees related to telecommunications services to support the system are the responsibility of the jurisdiction and are not allowable under this item. When utilizing FEMA program funds to build, upgrade, enhance, or replace communications systems, grantees and sub-grantees should develop a comprehensive interoperable communications plan before procurement decisions are made.

04AP-11-SAAS	Applications, Software as a Service	Sometimes referred to as "on-demand software", SAAS applications run on the provider's servers, delivering functionality via the internet to any device having connectivity and the required browser or interface. Access to the application is obtained via a service subscription rather than outright purchase, with all updates and configuration requirements handled by the service provider. Some example SAAS applications include equipment tracking and maintenance, intra-application communication among client devices, and specialized software such as plume modeling. Note that purchasers of SAAS should consider the security aspects of the planned usage, particularly availability and the protection of sensitive information stored remotely. Internet connectivity is required to utilize SAAS applications unless specific failover measures such as a "hybrid cloud" are available. In addition, data is stored remotely on vendor equipment. Use of SAAS for mission critical applications should be thoroughly vetted before implementation.	
05AU-00-TOKN	System, Remote Authentication	System used to provide enhanced remote authentication, usually consisting of a server, some synchronization scheme, and a device, token, or smartphone application.	
05EN-00-ECRP	Software, Encryption	Encryption software for protecting stored data files or email messages.	
05HS-00-MALW	Software, Malware/Anti-Virus Protection	Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments.	
05HS-00-PFWL	System, Personal Firewall	Personal firewall for operation on individual devices. Usually a software solution, but appliances are also available. See also: 05NP-00-FWAL.	
05NP-00-FWAL	Firewall, Network	Firewall (software or standalone appliance) for use in protecting networks. See also 05HS-00-PFWL.	
05NP-00-IDPS	System, Intrusion Detection/Prevention	Intrusion Detection and/or Prevention System (IDS, IPS) deployed at either host or network level to detect and/or prevent unauthorized or aberrant behavior on the network. Software and hardware (appliance) solutions exist. This replaces item 05NP-00-IDS and incorporates more recent prevention technology.	

06CP-01-PORT	Radio, Portable	Individual/portable radio transceivers.	This section includes equipment and systems that provide connectivity and electrical interoperability between local and interagency organizations to coordinate CBRNE response operations. When utilizing FEMA program funds in the category of Interoperable Communications Equipment to build, upgrade, enhance, or replace communications systems, grantees and sub-grantees should develop a comprehensive interoperable communications plan before procurement decisions are made. Grant funds may be used to cover only those services provided during the grant project period. Grantees are reminded that supplanting of previously planned or budgeted activities is strictly prohibited. Grantees should coordinate with their assigned FEMA preparedness officer to determine the appropriate allowable cost category for these purchases.
06CP-03-ICOM	Intercom	System for hands-free (wired or wireless) communication for limited numbers of personnel in close proximity, such as vehicle crew members. Includes systems designed for underwater use.	
06CP-03-PRAC	Accessories, Portable Radio	Speaker/microphone extensions to portable radios. Sometimes used within encapsulated/partially encapsulated suits, where restricted access to radio equipment impedes normal portable radio operations. Also includes programming/cloning cables.	This section includes equipment and systems that provide connectivity and electrical interoperability between local and interagency organizations to coordinate CBRNE response operations. When utilizing FEMA program funds in the category of Interoperable Communications Equipment to build, upgrade, enhance, or replace communications systems, grantees and sub-grantees should develop a comprehensive interoperable communications plan before procurement decisions are made. Grant funds may be used to cover only those services provided during the grant project period. Grantees are reminded that supplanting of previously planned or budgeted activities is strictly prohibited. Grantees should coordinate with their assigned FEMA preparedness officer to determine the appropriate allowable cost category for these purchases.
10GE-00-GENR	Generators	Generators, varying types and sizes, including gasoline, diesel, propane, natural gas, alternator, gas turbine powered devices, etc.	
10PE-00-UPS	Supply, Uninterruptible Power (UPS)	Systems that compensate for loss of power to serviced equipment for some period of time. May include short-duration battery devices, or standby generator devices for longer duration.	

13IT-00-ALRT	System, Alert/Notification	Alert and notification equipment that allows for real-time dissemination of information and intelligence among responders via equipment such as cellular phones, pagers, text messaging, etc. This functionality may also be obtainable via subscription as a cloud-based service using a web browser interface or a mobile app, as opposed to local software. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information.	Fees related to telecommunications services to support the system are the responsibility of the jurisdiction and are not allowable under this item. When utilizing FEMA program funds to build, upgrade, enhance, or replace communications systems, grantees and sub-grantees shoudl develop a comprehensive interoperable communications plan before procurement decisions are made.
14CI-00-COOP	System, Information Technology Contingency Operations	Back-up computer hardware, operating systems, data storage, and application software necessary to provide a working environment for contingency operations. May be a purchased remote service or a dedicated alternate operating site. This functionality may also be obtainable via subscription as a cloud-based service. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.
14EX-00-BCAN	Receptacles, Trash, Blast-Resistant	Blast-resistant trash receptacles.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities. No standard currently exists for these products. Grantees are advised to carefully review vendor specifications and test results prior to purchase.
14EX-00-BSIR	Systems, Building, Blast/Shock/Impact Resistant	Systems to mitigate damage from blasts, shocks, or impacts, such as column and surface wraps, wall coverings, breakage/shatter resistant glass, window wraps, and deflection shields.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.
14SW-01-ALRM	Systems/Sensors, Alarm	Systems and standalone sensors designed to detect access violations or intrusions using sensors such as door/window switches, motion sensors, acoustic sensors, seismic, and thermal sensors. May also include temperature sensors for critical areas.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.
14SW-01-ASTN	Network, Acoustic Sensor Triangulation	A network consisting of some number of deployed acoustic sensors and one or more processing nodes for data integration and analysis. Such networks can be "tuned" to one or more ranges of frequencies to detect sounds such as gunshots, heavy weapons discharge, explosions, MANPAD launches, vehicle noises, etc., and utilize acoustic triangulation to provide accurate location data. Such networks can be wired, wireless, or hybrid, and are capable of operation near critical infrastructure assets or in wide areas.Â	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.Â

14SW-01-DOOR	Doors and Gates, Impact Resistant	Reinforced doors and gates with increased resistance to external impact for increased physical security.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.
14SW-01-EXTM	System, Fire Extinguisher Monitoring	System for monitoring the presence and pressure of fixed-location fire extinguishers to ensure that they are usable and are not stolen for possible misuse.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.
14SW-01-LITE	Lighting, Area, Fixed	Fixed high-intensity lighting systems for improved visibility in areas such as building perimeters and surveillance zones.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.
14SW-01-PACS	System, Physical Access Control	Locking devices and entry systems for control of physical access to facilities.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.
14SW-01-SNSR	Sensors/Alarms, System and Infrastructure Monitoring, Standalone	Standalone sensors/alarms for use on critical systems or infrastructure items (security systems, power supplies, etc.) to provide warning when these systems fail or are near failure.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.
14SW-01-VIDA	Systems, Video Assessment, Security	Camera-based security systems utilizing standard, low light, or infrared technology.This functionality may also be obtainable via subscription as a cloud-based service using a web browser interface or a mobile app, with imagery stored in the cloud as opposed to local software and storage. However, special security considerations apply for data stored remotely, including evidentiary issues for stored video. See 04AP-11-SAAS for further information.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.For the Nonprofit Security Grant Program, license plate reader and facial recognition systems are not allowed, but systems to detect weapons through video analysis are allowed.
14SW-01-WALL	Barriers: Fences, Jersey Barriers	Obstacles designed to channel or halt pedestrian or vehicle-borne traffic in order to protect a physical asset or facility.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.
15SC-00-PPSS	Systems, Personnel/Package Screening	Hand-held or fixed systems such as walk-through magnetometers and conveyor-belt x-ray systems used to screen personnel and packages for hazardous materials/devices.	Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.
21GN-00-INST	Installation	Installation costs for authorized equipment purchased through FEMA grants.	
21GN-00-SHIP	Shipping	Shipping costs for equipment purchased with grant funding.	
21GN-00-STAX	Sales Tax	Sales tax on equipment purchased with grant funding.	

21GN-00-TRNG	Training	Training on CBRNE and cyber security equipment by vendors or local entities.	DHS encourages the use of Domestic Preparedness Equipment Technical Assistance Program (DPETAP) for equipment training; however, manufacturer/vendor equipment training, the cost of overtime to attend the training, and costs related to having vendors provide training on equipment to State and/or local units of government is allowed to facilitate the training on and fielding of equipment. Note that training expenses allowable under this item must be equipment-specific. Expenses for generic training or operations training (even if equipment is used during the training) are not allowable. For non-equipment-specific training, please see applicable training guidelines in the appropriate fiscal year's grant program guidance.