|  |  |  |  |
| --- | --- | --- | --- |
| **AEL/SEL Number** | **Title** | **Description** | **Examples:** |
| 030E-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.  Useful for crowd control or briefing incident personnel. | Microphones; amplifiers; loudspeakers and related equipment.  **Must provide justification as to WHY this is essential for your organization and how system would be used.** |
| 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 may 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. | Software and system to produce credentialing, name tags, badges.  **Must provide justification as to WHY this is essential for your organization and how system would be used.** |
| 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), the Integrated Public Alert and Warning System (IPAWS), and Wireless Emergency Alerts (WEA). | Sirens and Alert Systems.  **Must provide justification as to WHY this is essential for your organization and how system would be used.** |
| 04-AP-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. | Application Subscription Services (Contractual Services) for equipment tracking and communications.  Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds.  **Must provide justification as to WHY this is essential for your organization and how service would be used.** |
| 05-AU-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. | Remote Authentications. Although allowable, the MOHS has not funded this category with past funding.  **Must provide justification as to WHY this is essential for your organization and how system would be used.**    Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds. |
| 05EN-00-ECRP | Software, Encryption | Encryption software for protecting stored data files or email messages. | Encryption Software. Although allowable, the MOHS has not funded this category with past funding.  **Must provide justification as to WHY this is essential for your organization and how software would be used.**    Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds. |
| 05HS-00-MALW | Software, Malware/Antivirus Protection | Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments. | Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds.  **Must provide justification as to WHY this is essential for your organization and how software would be used.** |
| 05HS-00-PFWL | System, Personal Firewall | Personal firewall for operation on individual workstations. Usually a software solution, but appliances are also available | Personal Firewall System. Although allowable, the MOHS has not funded this category with past funding. Any computer systems should be for the entity and not for personal use.  **Must provide justification as to WHY this is essential for your organization and how system would be used.**    Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds.  **Must provide justification as to WHY this is essential for your organization and how system would be used.** |
| 05NP-00-FWAL | Firewall, Network | Firewall (software or standalone appliance) for use in protecting networks. | Network Firewall System. Although allowable, the MOHS has not funded this category with past funding.  **Must provide justification as to WHY this is essential for your organization and how system would be used.**    Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds. |
| 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. | Intrusion Systems. Although allowable, the MOHS has not funded this category with past funding.  **Must provide justification as to WHY this is essential for your organization and how system would be used.**    Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds. |
| 06CP-01-PORT | Radio, Portable | Individual/portable radio transceivers. | Portable Radio.  **Must provide justification as to WHY this is essential for your organization and how equipment would be used.** |
| 06-CC-02-PAGE | Services/Systems, Paging | Paging services/systems, 1-way text messaging. | Pagers. Although allowable, the MOHS has not funded this category with past funding.  **Must provide justification as to WHY this is essential for your organization and how services would be used.**    Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds. |
| 06CP-03-ICOM | Intercom | System for hands-free (wired or wireless) communication for limited numbers of personnel in proximity, such as vehicle crew members. Includes systems designed for underwater use. | Communication for limited numbers of personnel. Intercom systems.  **Must provide justification as to WHY this is essential for your organization and how system would be used.** |
| 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. | Speaker and Microphone Extensions for Portable Radio. Signal Boosters, headsets.  Although allowable, the MOHS has not funded this category with past funding.  **Must provide justification as to WHY this is essential for your organization and how equipment would be used.** |
| 10GE-00-GENR | Generators | Generators, varying types, and sizes, including gasoline, diesel, propane, natural gas, alternator, gas turbine powered devices, etc. | **Must provide justification as to WHY this is essential for your organization and how equipment would be used.** |
| 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. | Alert or notification systems. Could be cellular phones, pagers, text message devices or cloud services to notify the public.  **Must provide justification as to WHY this is essential for your organization and how system would be used.**    Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds. |
| 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. | Back up Systems and data storage in the event of a cyber attack or terrorist event. Creates a working environment for contingency of operations.  Subscription Services are only funded for (1) year and the period of performance for the grant.  **Must provide justification as to WHY this is essential for your organization and how system would be used.**  Agency must be able to show how the services will be able to continue without grant funds. |
| 14EX-00- BCAN | Receptacles, Trash, Blast- Resistant | Blast-resistant trash receptacles. | Trash receptacles that can withstand terrorism blasts. Although allowable, the MOHS has not funded this category with past funding.  **Must provide justification as to WHY this is essential for your organization and the Need for item.** |
| 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. | Column and Surface wraps, Wall coverings, shatter resistant glass, window wraps and shield.  Please NOTE: This is not to replace the windows of your organization.  **Must provide justification as to WHY this is essential for your organization and the Need for item.** |
| 14SW-01-ALRM | Systems/Sensors, Alarm | Systems and standalone sensors are 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. | Alarm systems can include **sensors** on doors, windows, motion sensors. Hard-wired and wireless systems available. Includes self-monitoring standalone sensors as well as integrated systems. May be integrated into access control system. Remote control and monitoring available via Cloud on smart phones and tablets as well as desktop systems.  Subscription Services are only funded for (1) year and the period of performance for the grant.  **Must provide justification as to WHY this is essential for your organization and how system would be used.**  Agency must be able to show how the services will be able to continue without grant funds. |
| 14SW-01-DOOR | Doors and Gates, Impact Resistant | Reinforced doors and gates with increased resistance to external impact for increased physical security. | Reinforced Doors and Gates.  Please NOTE: This is not to replace the doors and gates of your whole organization. Doors and Gates should be purchased only in areas that will need increased resistance and increased physical security.  **Must provide justification as to WHY this is essential for your organization and the Need for item.** |
| 14SW-01-LITE | Lighting, Area, Fixed | Fixed high-intensity lighting systems for improved visibility in areas such as building perimeters and surveillance zones. | Lighting for potential areas in need of high visibility. Wall or pole mounted. Motion detection lighting  Please NOTE: This is not to replace the current lighting for your organization. Lighting should be purchased only in areas that will need increased visibility and increased physical security.  **Must provide justification as to WHY this is essential for your organization and the Need for item.** |
| 14SW-01-PACS | System, Physical Access Control | Locking devices and entry systems for control of physical access to facilities | Locking devices and entry systems.  Please NOTE: This is not doors or doorways. Access controls are the access points to an area. This is not to be used for every door in your organization, only in areas for protection.  **Must provide justification as to WHY this is essential for your organization and the Need for item.** |
| 14SW-01-SIDP | Systems, Personnel Identification | Systems for positive identification of personnel as a prerequisite for entering restricted areas or accessing information systems.  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 purchasing software. However, special security considerations apply for data stored remotely. | Personnel identification systems are designed and installed for the primary purpose of ensuring that only authorized persons are allowed access to secure areas of a facility. Identification system to enter a building. Ex. Access Card; Pin Number or Fingerprint.  Subscription Services are only funded for (1) year and the period of performance for the grant.  **Must provide justification as to WHY this is essential for your organization and the Need for item.** |
| 14SW-01-SIDV | Systems, Vehicle Identification | Systems for identification and tracking of vehicles, ranging from decals to radio frequency identification (RFID) or other transponder or GPS-based devices.  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. Such services could use specialized vehicle sensors or reporting capabilities already built into the vehicle. However, special security considerations apply for data stored remotely. | Identification and Tracking System of Vehicles. Although allowable, the MOHS has not funded this category with past funding.  **Must provide justification as to WHY this is essential for your organization and how system would be used.**    Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds. |
| 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. | Security system. **Must provide justification as to WHY this is essential for your organization and how system would be used.**    Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds. |
| 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. | Video Camera Systems for recording activity.  Services are only purchased for (1) year and the period of performance for the grant.  Agency must be able to show how the services will be able to continue without grant funds. |
| 14SW-01-WALL | Barriers: Fences; Jersey Walls | Obstacles designed to channel or halt pedestrian or vehicle-borne traffic to protect a physical asset or facility. | Fencing and walls.  **Must provide justification as to WHY this is essential for your organization and how would be used.**  Please NOTE: Fencing should be measured and an accurate description of the fence the entity will need. This is not to be used as a decorate fence or to upgrade fencing for decorative use, but rather as a fence to prevent damage to your organization. |
| 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. | Metal Detectors.  **Must provide justification as to WHY this is essential for your organization and how system would be used.** |
| 21GN-00-INST | Installation | Installation costs for authorized equipment purchased through FEMA grants. | Installation of all equipment to be installed for Entity.  Please NOTE: Installation costs should be specific only to the items being installed for the federally funded project, not other projects. |
| 21GB-00-TRNG | Training | Training on CBRNE and cyber security equipment by vendors or local entities. | Training can be provided by MOHS for FREE. Although allowable, the MOHS encourages the use of available resources. |

Grantees should leverage private assets where appropriate when implementing security enhancements at privately-owned critical infrastructure facilities.