AEL – Authorized Equipment List Definitions

The Investment Justification has embedded a dropdown list of approved Authorized Equipment. The equipment and software offerings are described as:

03OE-03-MEGA: System, Public Address. Handheld or Mobile systems used for mass audio notification. This can include vehicle-mounted high powered speaker systems, or battery powered megaphone / public address systems with corded microphone.

03OE- 03 SIGN: Restricted access and caution warning signs that preprinted or field printable and can be various colors, sizes, and shapes. Examples can include traffic cones, other free-standing signage, mountable items, and signs and devices for individuals with disabilities and others with access and functional needs (e.g., programmable audible caution cones and scrolling marquis signs).

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 be required, functionality may also be obtainable via subscription as a cloud-based service, as opposed to purchasing software.

04AP-06-VIDA: Systems, Public Notification and Warning. Software, Video Analytics. Software, either local or cloud-based, that analyzes video input to detect/determine temporal and spatial events, either in real time or using archival video. Analytical priorities might include recognition or patterns (movement or arrangement or persons, vehicles, or other objects). For the NSGP, license plate reader and facial recognition software are not allowed, but software to detect weapons through video analysis is allowed.

04AP-09-ALRT: 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).

04AP-11-SAAS: Applications, Software as a Service. Sometimes referred to as "on-demand software," this application runs 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. *This item is limited to those services that support security systems such as access controls, camera networks, cybersecurity services or other critical infrastructure security.*

05AU-00-TOKN: System, Remote Authentication- Systems used to provide enhanced remote authentication, often consisting of a server or synchronization scheme and a device, token, or smartphone application.

05EN-00-ECRP: Software, Encryption. Consider 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 workstations. Usually there is a software solution, but appliances are also available.

05NP-00-FWAL: Firewall, Network firewall (software or standalone appliance) for use in protecting networks.

05NP-00-IDPS: System, Intrusion Detection/Prevention. Intrusion Detection and/or Prevention. This system is deployed at either host or network level to detect and/or prevent unauthorized or aberrant behavior on the network.

06CP-01-PORT: Radio, Portable. Individual/portable radio transceivers and alerts.

06CP-01-REPT: Repeater. Electronic device that receives a weak or low-level signal and retransmits that signal to extend usable range.

06CC-02-PAGE: Services/Systems. Paging services/systems, Paging services/systems/applications; one-way text messaging for notifications or alerts.

06CP-03-ICOM: Intercom. System for hands-free (wired or wireless) communication for limited numbers of personnel in close proximity to receive alerts or notifications.

06CP-03-PRAC: Accessories, Portable Radio. Speaker/microphone extensions to portable radios.

10GE-00-GENR: Generators. Generators (gasoline, diesel, propane, natural gas, etc.) and their required installation materials, including 10PE-00-PTSW (a power switch) if not already included, to support a redundant power supply for security systems, alarms, lighting, and other physical security/cybersecurity infrastructure or systems.

13IT-00-ALRT: System, Alert/Notification. Alert/notification software that allows for real-time dissemination of information for situational awareness or alerts among a group via means such as smartphones, landlines, pagers, etc. This item may also be a subscription cloud-based service using a web browser interface or a mobile application instead of a software.

10PE-00-UPS: Supply, Uninterruptible Power (UPS). Systems that compensate for power loss to serviced equipment (e.g., short-duration battery devices, standby generator devices for longer duration).

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 as a remote service or a dedicated alternate operating site.

14EX-00-BCAN: Receptacles, Trash, Blast-Resistant. Blast-resistant trash receptacles.

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.

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.

14SW 01 ASTN: Network, Acoustic Sensor Triangulation. Network of deployed acoustic sensors and one or more processing nodes for data integration and analysis. Such networks can be set to one or more ranges of frequencies to detect sounds such as gunshots, heavy weapons discharge, explosions, man-portable air defense system 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.

14SW-01-DOOR: Doors and Gates, Impact Resistant. Reinforced doors and gates with increased resistance to external impact for increased physical security.

14SW-01-LITE: Lighting, Area, Fixed. Fixed high-intensity lighting systems for improved visibility in areas such as building perimeters, parking lots, and other critical zones to increase physical security.

14SW-01-PACS: System, Physical Access Control. Locking devices and entry systems for control of physical access to facilities.

14SW-01-SIDP: Systems, Personnel Identification. Systems for positive identification of personnel as a prerequisite for entering restricted areas or accessing information systems.

14SW-01-SIDV: Systems, Vehicle Identification. Systems for identification of vehicles, ranging from decals to radio frequency identification or other transponder devices. (License plate reader and facial recognition software are NOT allowed.)

14SW-01-SNSR: Sensors/Alarms, System and Infrastructure Monitoring, Standalone. Standalone sensors/alarms for use on critical systems or infrastructure items (e.g., security systems, power supplies, etc.) to provide warning when these systems fail or are near failure.

14SW-01-VIDA: Systems, Video Assessment, Security. Camera-based security systems utilizing standard, low light, or infrared technology. (License plate reader and facial recognition software are NOT allowed.)

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 such as barriers, bollards, planters, benches etc. (Earthen barriers, berms, trees, or other botanical obstacles are NOT allowed.)

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.

21GN-00-INST: Installation. Installation costs for authorized equipment purchased through FEMA grants.

21GN-00-TRNG: Training. Training on CBRNE and cyber security equipment by vendors or local entities.

Contract Security: Private Contact Security Personnel/Guards. The program is limited to federal, state, county, or municipal law enforcement officers, active special law enforcement officers appointed pursuant to P.L.1985, c.439, or security officers registered pursuant to P.L.2004, c.134. This funding is exclusively for the hiring of security personnel. It may **not** be used to supplant expenses for current security personnel but may be used to **supplement** additional security personnel needs based on identified risk. Security agencies must be currently registered with the State of New Jersey. Individual security personnel/law enforcement officers must be formally trained and authorized in accordance with the law previously mentioned in this presentation.

M&A: Management and Administration (M&A)

Planning...funding may be used for security or emergency planning expenses and the materials required to conduct planning activities. Planning must be related to the protection of the facility and the people within the facility. Examples of planning activities allowable under this program include:

- Development and enhancement of security plans and protocols.

- Development or further strengthening of security assessments.

- Emergency contingency plans.

• Evacuation/Shelter-in-place plans.

Exercise...funding may be used to conduct security-related exercises. This includes costs related to planning the exercise, meeting space and other meeting costs, facilitation costs, materials and supplies and documentation. A clear way to distinguish Exercise a to test a plan, with any physical response is an "exercise" Planning is written protocols in place for incidents or evacuations.