NC Department of Public Safety
EMERGENCY MANAGEMENT

Josh Stein, Governor

Eddie M. Buffaloe Jr., Secretary
William C. Ray, Director

MEMORANDUM

TO: Derek Dorazio

FROM: Greg Hauser

DATE: February 6, 2025

SUBJECT: Requirements for Grant Funded Communications Equipment or Capabilities

To align communications technologies with current statewide communications plans, systems, networks, strategies and emerging technologies, the North Carolina State Interoperability Executive Committee (SIEC) requires that purchases made with U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA) federal financial assistance meet requirements. These sources of funding include the Emergency Management Performance Grant (EMPG) and the Homeland Security Grant (HSGP). The below requirements must also be met for those purchases made with NCEM Capacity Building Competitive Grant (CBCG), State & Local Cybersecurity Grant Program (SLCGP), and Emergency Operations Center Grant Program (EOCGP) funds. Included are the equipment identifiers as listed on the FEMA Authorized Equipment List (AEL) that are allowable, where applicable. Awardees should log on to the FEMA website to verify that the equipment below they wish to purchase is allowable under the above grant program.
https://www.fema.gov/grants/tools/authorized-equipment-list

700/800 MHz Radio purchases (06CP-01-BASE, 06CP-01-MOBL, 06CP-01-PORT)

Radio purchases can be classified into three parts: portable (handheld), mobile (vehicular/desktop) or console/consolette (software/infrastructure). These radios must appear on the current VIPER Approved Radio List, and have the following capabilities, i.e., the feature must be purchased and present in the radio:

- Capable of operating on a P25 radio system/network
- Capable of operating in a P25 Phase II (TDMA) environment
- Capable of passing and receiving AES/256-bit encryption
- Capable of utilizing more than one encryption key

Further information is available at:
https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment

All radios purchased using the above noted grant sources shall have the VIPER statewide template in them. This template was approved by the SIEC on June 6th, 2021 and revised on April 15th, 2024.

If a grant recipient chooses to operate in an encrypted environment, all radios purchased using the above noted grant sources shall follow the SIEC Interoperable Radio Encryption Standard Operating Guideline approved on May 28th, 2020 and revised on April 9th, 2023.

Non 700/800 MHz radio purchases (06CP-01-BASE, 06CP-01-MOBL, 06CP-01-PORT)

Non 700/800 MHz radios (UHF/VHF) are allowable provided they are included on the below list of grant eligible equipment.

https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment

If a radio purchase is requested for other, non-P25 networks the following are **NOT** eligible:

- Wouxun handheld or mobile radios (multiband).
- Baofeng handheld or mobile radios (multiband).
- Any other wireless device outlined in the Federal Communication Commission's (FCC) "List of equipment and services covered in section 2 of the Secure Networks Act" This list is a result of the passage of *H.R.5515 - John S. McCain National Defense Authorization Act in 2019.* Further information can be found at https://www.fcc.gov/supplychain/coveredlist.

Public Alerting Software Platforms (04AP-09-ALRT)

Public alerting software platforms are a means of alerting citizens of emergencies. There are two distinct functions that a software platform provides. There is a citizen sign up option for notifications and a wireless emergency alerting (WEA) function. The WEA function alerts smartphones and devices based on geographic location through the Integrated Public Alert and Warning System (IPAWS). Please make sure the purchasing agency is a North Carolina/FEMA approved public alerting authority (PAA) or is in the process of obtaining the PAA status **If purchasing or subscribing to software, it must be identified on the attached *"List of Alert Software Providers (AOSP) That Have Successfully Demonstrated Their IPAWS Capabilities."***

Voice Gateway Devices (06CP-02-BRDG)

Gateway devices are used to bridge disparate voice sources together to create a single line of communications. This can include radio, voice over IP, smart device application, etc. These devices are **NOT** allowed to be permanently mounted at Public Safety Answering Points (PSAP), tower sites or network rooms to permanently patch disparate radio systems. Written permission **must** be obtained from all system administrators authorizing the intended use of the gateway device on the system.

Items not included or referenced in this document must be clearly identified to ensure that interoperability, physical security, and cybersecurity priorities are followed. Examples include, but are not limited to:

- Smart device applications that integrate into first responder communications networks.

- Infrastructure equipment that allows for the integration of smart device applications.
- Equipment that uses shared radio frequency (RF) spectrum to create mesh networks.

Information Sharing and Collaboration Applications (04AP-11-SAAS)

Information sharing and collaboration applications are becoming vital to planning and incident-based decision making amongst public safety agencies. The SIEC recognizes the importance of these tools but cautions public safety agencies that some publicly accessible tools may be vulnerable to cyber threats and violate public records policies and/or laws. Awardees are welcomed to purchase information sharing and collaboration applications if they meet the below requirements:

- The application must meet the National Institute of Standards and Technology (NIST) 800-53 standard for security and privacy controls for information systems and organizations. This includes meeting the Federal Risk and Authorization Management Program (FedRAMP) moderate standard. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- The agency/user must be able to retrieve achieved data to meet agency public records and retention policies/laws.

Questions can be directed to the SIEC via the NCEM Communications Branch for passage to the SIEC Chair and Vice-Chair.

WR/gh