



ISOO Notice 2020-01: COVID-19 guidelines and alternative operating methods for alarm monitoring industry

May 12, 2020

References

- a. 32 CFR 2001, Classified National Security Information
- b. 32 CFR 2004, The National Industrial Security Program (NISP) directive
- c. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM)
- d. UL-2050, National Industrial Security Systems for the Protection of Classified Information
- e. UL-827, Standards for Central Station Alarm Services
- f. UL Statement on Certifications to the US Alarm Monitoring Industry and Virtual Workplace Guidelines, March 16, 2020

This guidance document is binding on agency actions as authorized under applicable statute, executive order, regulation, or similar authority. This guidance does not have the force and effect of law on, and is not meant to bind, the public, except as authorized by law or regulation or as incorporated into a contract.

Background

The NISPOM (reference c) specifies minimum standards for an approved intrusion detection system (IDS) as a supplemental protection measure for Top Secret and Secret material. (5-900.) One of the requirements for such systems is that it must be connected to, and monitored by, a central monitoring station. (5-900.) Additional provisions in section 9 of the NISPOM tie requirements to Underwriter's Laboratories (UL) standards in UL-2050 (reference d), which further directs standards in UL-827 (reference e). UL-827 sets out on-site monitoring station requirements.

During the COVID-19 pandemic, agencies and industry have been asking questions about manning at Certified Central Stations (*i.e.*, companies that provide alarm monitoring for cleared contractors in the National Industrial Security Program (NISP), and, in some cases, for Federal agencies) in light of COVID-19 response mandates from authorities (affecting covered facilities in the U.S. and overseas).

Guidance

ISOO, in its oversight role regarding the NISP, encourages Cognizant Security Agencies (CSAs) to follow the current guidelines set forth in 32 CFR 2001 and in the NISPOM for emergency situations.

32 CFR 2001.52, Emergency authority, paragraph (a), states that "agency heads or any designee may prescribe special provisions for the dissemination, transmission, safeguarding, and destruction of classified information during certain emergency situations." The COVID-19 pandemic qualifies as such an emergency situation, particularly during the period when state and national authorities issue requirements for businesses to close, people to remain at home, social distancing, and similar restrictions that impact normal manning and facility operations.

32 CFR 2001.40(b) also states, "... agency heads or their designee(s) may adopt alternative measures, using risk management principles, to protect against loss or unauthorized disclosure when necessary to meet operational requirements. When alternative measures are used for other than temporary, unique situations, the alternative measures shall be documented and provided to the Director of ISOO. Upon request, the description shall be provided to any other agency with which classified information or secure facilities are shared. In all cases, the alternative measures shall provide protection sufficient to reasonably deter and detect loss or unauthorized disclosure. Risk management factors considered will include sensitivity, value, and crucial nature of the information; analysis of known and anticipated threats; vulnerability; and countermeasure benefits versus cost."

In addition, the NISPOM, at 5-104, Emergency procedures, states that "Contractors shall develop procedures for safeguarding classified material in emergency situations. The procedures shall be as simple and practical as possible and should be adaptable to any type of emergency that may reasonably arise. Contractors shall promptly report to the CSA any emergency situation that renders the facility incapable of safeguarding classified material." More particularly in this case, the NISPOM, at 5-906(a), states that "If the requirements [for the IDS and monitoring stations] cannot be met, the contractor may request CSA approval for an alarm system meeting one of the conditions listed [in 5-906]. CSA approval will be documented on the Alarm Description Form."

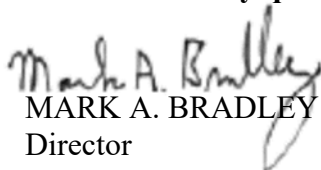
However, if the emergency situation does not allow for an alarm system meeting one of the conditions in 5-906 of the NISPOM, the CSA's emergency authority permits them to approve other measures.

Emergency circumstances such as the COVID-19 response may prevent contractors (or equivalent entities) from complying with the UL-827/UL-2050 standards for staffing and monitoring a UL Certified Central Station. In such cases, contractors/entities must discuss the situation and any proposed deviations from UL-2050/827 standards with the relevant CSA with jurisdiction over the contractor/entity and the type of classified information involved, as well as with the Government Contracting Activity (GCA).

In March 2020, in response to the COVID-19 pandemic, UL issued a statement (reference f) acknowledging potential issues with regard to monitoring a station with on-site manning, and setting out guidelines for remote, or virtual, monitoring. In circumstances in which personnel are at an increased COVID-19 risk on-site, and alternative options are not available to mitigate such risk, CSAs may choose to permit such remote, or virtual, monitoring, pursuant to their authority above. CSAs may also establish additional or alternative requirements to those set out by the UL statement.

ISOO encourages monitoring stations to make contingency plans for operating in emergency environments. Monitoring stations must document when they begin operating under such alternate procedures. Contractors/entities should contact the applicable Federal Government customer (the agency that would levy any additional requirements) regarding alarm systems for SAP or SCI to determine if there are any additional measures they will require for that information.

Please direct any questions regarding this ISOO Notice to isoo@nara.gov.


MARK A. BRADLEY
Director