



DEPARTMENT OF THE NAVY  
OFFICE OF THE JUDGE ADVOCATE GENERAL  
1322 PATTERSON AVENUE SE, SUITE 3000  
WASHINGTON NAVY YARD DC 20374-5066

JAG/COMNAVLEGSVCCOMINST 5530.2D CH-4

Code 67  
OCT 27 2019

JAG/COMNAVLEGSVCCOM INSTRUCTION 5530.2D CHANGE TRANSMITTAL 4

Subj: OFFICE OF THE JUDGE ADVOCATE GENERAL AND NAVAL LEGAL SERVICE  
COMMAND PHYSICAL SECURITY PROGRAM

Ref: (f) SECNAVINST 5430.107A

1. Purpose. To transmit a new page 14, promulgating a revised firearms policy and update reference (f).
2. Action. Remove page 14 of the instruction and insert enclosure (1).

*D. E. Crandall*  
D. E. CRANDALL  
Commander, Naval Legal Service Command

*John G. Hannink*  
JOHN G. HANNINK  
Judge Advocate General

Releasability and Distribution:

This instruction is cleared for public release and is available electronically via the OJAG Website  
<http://www.jag.navy.mil>.



DEPARTMENT OF THE NAVY  
OFFICE OF THE JUDGE ADVOCATE GENERAL  
1322 PATTERSON AVENUE SE, SUITE 3000  
WASHINGTON NAVY YARD DC 20374-5066

JAG/COMNAVLEGSVCCOMINST 5530.2D

Code 67

JUN 08 2017

JAG/COMNAVLEGSVCCOM INSTRUCTION 5530.2D

Subj: OFFICE OF THE JUDGE ADVOCATE GENERAL AND NAVAL LEGAL SERVICE  
COMMAND PHYSICAL SECURITY PROGRAM

Ref: (a) OPNAVINST 5530.14E (Series)  
(b) U.S. Navy Regulations 0825, 0826  
(c) COMNAVLEGSVCCOMINST 5800.1G  
(d) JAG Memorandum of Agreement with CNIC 5800 Ser N00/12U71536 of 5 Nov 12  
(e) U.S. Courts Design Guide

Encl: (1) OJAG Physical Security Organizational Chart  
(2) Risk Assessment with Instructions  
(3) Sample Warning Placard  
(4) Sample Visitor Log  
(5) Sample Visitor Badges  
(6) Sample Physical Security Quarterly Report  
(7) Sample Physical Security Waiver Request

1. Purpose. To implement physical security policy and procedures for the Office of the Judge Advocate General (OJAG) and Naval Legal Service Command (NLSC) commands and activities, including NLSC court facilities. A secure environment, free from the threat of physical harm and intimidation, is essential for NLSC mission accomplishment. Reference (a) provides guidance and requirements for the Navy's physical security and law enforcement program. Reference (b) directs that Commanding Officers shall require personnel to be instructed and trained in all applicable safety precautions and procedures, that those precautions and procedures are complied with, and that personnel, equipment, material and documents are safeguarded. In accordance with reference (c), this instruction provides additional security requirements designed to detect, deter and defeat the most likely security threats to certain NLSC facilities providing client/customer-centric legal services. This new instruction is a complete revision of the previous instruction and must be reviewed in its entirety. Major changes are summarized below.

a. This instruction provides physical security standards and/or best practices for OJAG and NLSC activities and facilities, with or without court facilities.

b. This instruction includes a program organizational chart, sample placard, sample visitor log, sample visitor badges, sample quarterly report, and sample waiver request. It also includes a revised guide for risk assessments.

JUN 08 2017

c. This instruction eliminates annual certification and "tier" ratings for courthouses and courtrooms. It establishes a minimum security posture and requirements for certain NLSC activities and, for military justice proceedings, risk assessments and corresponding security plans.

d. This instruction defines roles and responsibilities of OJAG and NLSC personnel.

e. This instruction streamlines and clarifies the completion of initial risk assessments, as well as the routing of security plans, quarterly physical security reports and waiver requests.

2. Cancellation. COMNAVLEGSVCCOMINST 5530.2C.

3. Scope and Applicability

a. This instruction applies to all OJAG and NLSC facilities, including offices, occupied by personnel assigned to the Navy and Marine Corps Trial Judiciary (NMCTJ), Defense Service Offices (DSO), Region Legal Service Offices (RLSO), Victims' Legal Counsel (VLC) Program, Navy-Marine Corps Appellate Review Activity, and Naval Justice School (NJS).

b. OJAG executes a special mission to support Echelon III NLSC field activities in the area of civil law, military justice, operations, and management. OJAG refers to the combined OJAG/NLSC Headquarters activity, which includes all OJAG/NLSC offices and units at the Washington Navy Yard, the Pentagon, and field activities such as the Claims and Tort Litigation activities in Norfolk, Virginia; Pensacola, Florida; and San Diego, California, and the Judge Advocate General's Corps Consolidated Administrative Branch office. Because the standards in this instruction are primarily focused on potential security threats that may arise in the provision of client-centric and/or customer-service-based legal services (e.g., military justice, defense services, legal assistance, and command services), OJAG is not subject to the requirements outlined in paragraphs 5 and 6 of this instruction, with the exception of paragraph 5(a)(3)(d). OJAG is required to comply with reference (a), and the spirit and intent of this instruction, in order to ensure the physical security of its locations and safety of its personnel. OJAG personnel are required to participate in, and comply with, host installation physical security programs, and to report relevant issues and deficiencies through their chain of command to Code 67 for action and resolution.

c. NJS executes a unique training mission, likewise not primarily focused on potential security threats that may arise in the provision of client-centric and/or customer-service-based legal services. Therefore, NJS is not subject to the requirements outlined in paragraphs 5 and 6 of this instruction, with the exception of paragraph 5(a)(3)(e). NJS is required to comply with references (a) through (c), and the spirit and intent of this instruction, in order to ensure the physical security of its locations and safety of its personnel. NJS personnel are required to participate in, and comply with, host installation physical security programs.

d. This instruction applies to facilities in which OJAG or NLSC is the sole tenant, or to dedicated portions of facilities in which OJAG or NLSC has exclusive occupation and use. It does not apply to offices in which OJAG or NLSC personnel work, but are not physically located

JUN 08 2017

in an OJAG or NLSC facility (e.g., installation Staff Judge Advocate who is attached to a RLSC and a tenant of a non-NLSC building).

e. A “military justice proceeding” involves any pre-trial, trial or post-trial session or proceeding associated with a special or general court-martial, including Uniform Code of Military Justice (UCMJ) Article 32 preliminary hearings, sessions held under UCMJ Article 39(a), and oral arguments before the Navy-Marine Corps Court of Criminal Appeals. Absent unique circumstances to be determined on a case-by-case basis by the Assistant Judge Advocate General, Operations and Management, a “military justice proceeding” does not include summary courts-martial, UCMJ Article 802 conferences, non-judicial punishment hearings, boards of inquiry, administrative separation boards, or legal assistance appointments.

f. In accordance with reference (c), all NLSC personnel are assigned responsibility for the physical security of NLSC command, detachment, and branch office spaces. Commanding Officers (COs) are responsible for ensuring all NLSC spaces and government property are protected and used only for authorized purposes [references (a) through (c)]. An organizational chart denoting command relationships and responsibilities is provided in enclosure (1).

#### 4. Responsibilities

##### a. Commander, Naval Legal Service Command (CNLSC)

(1) Maintain ultimate responsibility for ensuring the safety and security of NLSC commands, activities, and personnel in accordance with references (a) through (c).

(2) Ensure NLSC commands are properly resourced to execute the security requirements of references (a), (c), and (d) and this instruction.

(3) Ensure a review of implementation and compliance with this instruction is part of the Article 6 inspection process.

##### b. Assistant Judge Advocate General, Operations and Management (AJAG 06)

(1) Exercise oversight of the OJAG/NLSC physical security program.

(2) Act in the absence of CNLSC on matters pertaining to NLSC physical security.

(3) Approve or disapprove physical security equipment requests from NLSC COs and AJAG, Military Justice (AJAG 02), in accordance with paragraph 5.

(4) Approve or disapprove, in coordination with the AJAG, Chief Judge (AJAG 05), firearm exception requests from military judges, in accordance with paragraph 5.

(5) Approve or disapprove security mitigation plans for “high” risk military justice proceedings in NLSC facilities, and acknowledge notification of “medium” risk proceedings, in accordance with paragraph 5.



JUN 08 2017

(6) Review quarterly physical security reports received from NLSC commands and AJAG 02, in accordance with paragraph 6.

(7) Approve or disapprove requested waivers to this instruction, in accordance with paragraph 6.

(8) Determine the area of responsibility (AOR) for physical security specialists, and promulgate such determinations through a notice.

c. Director, Code 67 (Technology, Operations, and Plans) (Code 67)

(1) Serve as the officer primarily responsible for the overall administration of the OJAG/NLSC Physical Security Program and ensure program requirements are met, including facility requirements. Coordinate with OJAG, Code 64 (Fiscal and Resource Services); Commander, Navy Installations Command (CNIC); and Naval Criminal Investigative Service (NCIS), as required.

(2) Provide guidance and direction to Physical Security Specialists and ensure that they are periodically trained as required in order to execute their functions under this instruction.

(3) Designate, in writing, an OJAG Physical Security Officer responsible for implementing this instruction and the requirements of references (a) and (b).

(4) Ensure an annual physical security assessment is conducted by a CNIC representative or by an OJAG Physical Security Specialist for each NLSC facility under the direct cognizance of COS-RLSO, COS-DSO, Navy-Marine Corps Appellate Review Activity and NJS, pursuant to references (a), (c), and (d). In the event that no CNIC representative or OJAG Physical Security Specialist is available, coordinate with NCIS for Security Training, Assistance and Assessment Team (STAAT) support of annual security assessments.

(5) Receive, review and route to AJAG 06 all physical security equipment requests from NLSC COs, NJS CO, and AJAG 02, in accordance with paragraph 5.

(6) Receive, review and route to AJAG 06 all firearm exception requests from military judges, in accordance with paragraph 5.

(7) Receive, review and route to AJAG 06 all "high" risk assessments and corresponding security plans, as well as notification of "medium" risk proceedings, in accordance with paragraph 5.

(8) Receive, review and route to AJAG 06 all quarterly physical security reports, in accordance with paragraph 6.

(9) Receive, review and make recommendations upon requested waivers to this instruction, in accordance with paragraph 6.

JUN 08 2017

(10) In collaboration with NJS CO, provide each NJS location with facilities, equipment acquisition, and financial support and resourcing, as required.

(11) In collaboration with NJS CO, provide each NJS location with the support and resourcing of a NLSC physical security specialist, physical security training, and other similar training, as required.

(12) In collaboration with NJS CO, provide each NJS location with support and resourcing for on-site physical security assessments and assessment reports, at least annually, or as required or as requested by the NJS CO.

(13) Consult with CNIC and NCIS Threat Mitigation Unit (TMU) when notified of inappropriate communications or threats against NLSC or NMCTJ personnel, or when a situation occurs posing a potential security threat. In the case of threatening or inappropriate contacts of judiciary personnel, also coordinate with the CJDON and Circuit Military Judge.

(14) Maintain records of NLSC Physical Security Program implementation, review, and compliance.

d. NLSC Chiefs of Staff

(1) Chief of Staff, Region Legal Service Offices; Chief of Staff, Defense Service Offices (COS-DSO); and Chief of Staff, Victims' Legal Counsel Program (COS-VLCP) shall coordinate with each other, and with the Chief Judge of the Department of the Navy and Code 67 to provide and implement additional policy and guidance consistent with this instruction.

(2) COS-DSO shall review physical security mitigation measures for military justice proceedings in non-NLSC court facilities involving DSO personnel only, and forward concerns of inadequate security measures to AJAG 06 via Code 67.

(3) Understanding that many VLC offices are not located in NLSC facilities, but that VLC frequently participate in proceedings in NLSC facilities, COS-VLCP shall serve as the officer primarily responsible for ensuring that VLC exercise sound judgment and full participation in RLSO or DSO security procedures, as appropriate, to deter, detect and defeat security threats. Given a VLC's unique position, COS-VLCP shall ensure that VLC coordinate with RLSO and DSO personnel to appropriately address security threats related to the VLC client's participation in proceedings (e.g., a protective order which names the VLC client as the protected party).

e. Region Legal Service Office, Commanding Officer (RLSO CO)

(1) Serve as the officer primarily responsible for the physical security of RLSO facilities and personnel and NLSC court facilities and personnel under their cognizance. Where RLSO and DSO activities are located within the same facility, the RLSO CO will be the authority responsible for physical security of that facility, and shall coordinate with the DSO CO on physical security issues.

(2) Develop standard operating procedures (SOP) to implement a physical security program in accordance with this instruction and references (a) through (d), in coordination with CNIC and DSO COs where applicable. Provide a copy of the SOP to Code 67.

(3) Designate, in writing, a command physical security officer responsible for implementing this instruction and the requirements of references (a) and (b). Notify the cognizant Circuit Military Judge, DSO CO, and Code 67.

(4) Assign an assistant physical security officer to assist the command physical security officer. Notify the cognizant Circuit Military Judge, DSO CO, and Code 67.

(5) In accordance with paragraph 5, ensure a risk assessment is conducted prior to any military justice proceeding under their cognizance. See enclosure (2).

(6) For "high" and "medium" risk military justice proceedings, coordinate the development of security plans with the local NCIS Special Agent in Charge (SAC), Region Security Office (RSO), or Installation Security Office (ISO).

(7) In accordance with paragraph 5, submit written security plans of "high" risk proceedings to AJAG 06, via Code 67, for approval.

(8) Approve security plans for proceedings assessed as "medium" or "low" risk, and in accordance with paragraph 5, notify AJAG 06, via Code 67 of any "medium" risk proceedings.

(9) Provide facility physical security reports as required by this instruction. Commanding officers are authorized and encouraged to raise physical security concerns to the AJAG 06, via Code 67, at any time, regardless of the timelines for submission of periodic reports.

(10) Where applicable, submit security mitigation measures to AJAG 06, via Code 67, in accordance with this instruction.

(11) Where applicable, submit requests, including equipment and waiver requests, to AJAG 06, via Code 67, in accordance with this instruction.

(12) Inform Code 67 and the local NCIS TMU when any RLSO, trial judiciary or VLC personnel receives an inappropriate communication or threat as a result of their official duties, or when a situation occurs that poses or posed a security threat.

(13) In coordination with the OJAG Facilities Officer, submit project funding requests and supporting documentation for unfunded security requirements and other facilities-related matters to Code 67 for approval and execution.

(14) Coordinate with the cognizant Circuit Military Judge, local judiciary, cognizant DSO CO, NCIS SAC, CNIC, RSO or ISO, and Code 67, as appropriate, to implement this program.

JUN 08 2017

f. Defense Service Office, Commanding Officer (DSO CO)

(1) Serve as the officer primarily responsible for the physical security of DSO facilities and personnel under their cognizance except where RLSO and DSO facilities are located in the same facility, and, resources permitting, provide support consistent with this instruction upon request from the cognizant RLSO CO and when directed by COS-DSO. Where RLSO and DSO activities are located within the same facility, in accordance with paragraph 4.e.(1) of this instruction, the DSO CO shall coordinate with the RLSO CO on physical security issues.

(2) Develop SOPs to implement a physical security program in accordance with this instruction and references (a) through (d), in coordination with the RLSO CO where applicable, and provide a copy of the SOP to Code 67.

(3) Designate, in writing, a command physical security officer responsible for implementing this instruction. Notify the cognizant Circuit Military Judge, RLSO CO, and Code 67.

(4) In accordance with paragraph 5, ensure a risk assessment is conducted prior to any military justice proceeding under their cognizance that is held in a non-NLSC facility. See enclosure (2).

(5) Where applicable, submit requests, including equipment and waiver requests, to AJAG 06, via Code 67, in accordance with this instruction.

(6) Provide physical security reports as required by this instruction. Commanding officers are authorized and encouraged to raise physical security concerns to the AJAG 06, via Code 67, at any time, regardless of the timelines for submission of periodic reports.

(7) Inform Code 67 and the local NCIS TMU when any DSO personnel receive an inappropriate communication or threat as a result of their official duties, or when a situation occurs that poses or posed a security threat.

(8) In coordination with the OJAG Facilities Officer, submit project funding requests for unfunded security requirements and other facilities-related matters to Code 67 for approval and execution.

(9) Coordinate with the cognizant Circuit Military Judge, local judiciary, cognizant RLSO CO, NCIS SAC, CNIC, RSO or ISO, and Code 67, as appropriate, to implement this program.

g. AJAG 02 (Military Justice)

(1) Serve as the officer primarily responsible for the physical security of facilities and personnel in Building 58 of the Washington Navy Yard.

(2) Comply with responsibilities assigned to RLSO CO, as detailed in this instruction, for all activities and proceedings that involve facilities and personnel in Building 58 of the Washington Navy Yard.

JUN 08 2017

(3) Report relevant physical security issues and deficiencies directly to Code 67 for action and resolution.

h. Naval Justice School Commanding Officer (NJS CO)

(1) Serve as the officer primarily responsible for the physical security of NJS personnel and facilities for the NJS headquarters and detachments, consistent with the spirit and intent of this instruction, and references (a) through (c). Because the Commander/Commandant of The Judge Advocate General's Legal Center and School (TJAGLCS) in Charlottesville, Virginia, is primarily responsible for the security of NJS assets located in that facility, the NJS CO will ensure NJS assets at TJAGLCS comply with security requirements as set forth by its Office of the Dean.

(2) Communicate and coordinate with Code 67, as required, to assess physical security requirements unique to the NJS mission and facilities, and to execute necessary functions and measures to ensure adequate physical security. This collaboration includes, but is not limited to, issues related to facilities, equipment, funding, training, and on-site assessments. Maintain open lines of communication with AJAG 06, via Code 67, for physical security matters, as necessary.

(3) Develop appropriate physical security plans for each NJS location, and forward such plans to Code 67.

(4) In collaboration with Code 67, ensure that periodic physical security training, and any other similar required training, (e.g., Antiterrorism/Force Protection), is provided to all NJS personnel.

(5) In collaboration with Code 67, ensure that on-site physical security assessments of all NJS locations are completed at least annually, or as required or as requested by Director, Code 67, and provide endorsement on such physical security assessment reports.

(6) Designate, in writing, a command physical security officer responsible for implementing this instruction and the requirements of reference (a).

(7) In accordance with paragraph 5(a)(3)(e), determine appropriate security measures and procedures, at all NJS locations, for building access by visitors.

i. Physical Security Specialist

(1) Provide physical security to all NLSC facilities in his/her AOR, whether primarily a RLSO, DSO or NJS controlled facility, by providing guidance and expertise to the appropriate Command Physical Security Officers in the daily implementation of command physical security programs.

(2) Provide orientation and refresher security training materials specific to security personnel working in NLSC facilities in his/her AOR, as well as command-wide security training materials for all staff members working in NLSC facilities in the AOR, and maintain records of

such training. Security education programs shall include, but are not limited to, general security safety and awareness, theft prevention, and installation-specific security procedures.

(3) Ensure security screenings and sweeps are conducted properly by security personnel.

(4) Provide oversight of monitoring, maintenance and testing of all physical security systems and alarms in NLSC facilities in his/her AOR, and maintain records of such maintenance and testing.

(5) Plan and execute security drills, and assist with the completion of written after-action reports on such drills.

(6) Assist RLSO, DSO and NJS COs with the preparation of facility physical security reports and security plans, as required.

(7) Coordinate as required with RLSO and DSO COs to provide physical security support for military justice proceedings held in non-NLSC facilities.

(8) Coordinate, as required, with Code 67, CNIC and NCIS STAAT to ensure completion of an annual security assessment for each NLSC facility within the respective AOR.

(9) Liaise with local public works, Naval Facilities Engineering Command staff, and the Code 67 Facilities Officer to identify security-related items in need of maintenance or repair, and initiate and track required corrective action, service calls, and work orders.

(10) Report all physical security incidents, violations, vulnerabilities and deficiencies to Director, Code 67, in order to implement appropriate mitigation measures and required investigations.

(11) Coordinate with the cognizant Circuit Military Judge or local judiciary, the cognizant RLSO/DSO/NJS CO, RSO or ISO, CNIC, host installation, other local NLSC personnel (e.g., VLC, Trial Counsel Assistance Program, Defense Counsel Assistance Program), and Code 67, as appropriate, to implement this program.

(12) Maintain records from each command supported of physical security maintenance and testing, command training, physical security drills, and security incidents/concerns, and be prepared to support Command Physical Security Officers in preparation for Article 6 inspections.

j. Command Physical Security Officer

(1) Serve as the officer primarily responsible for overseeing the daily implementation of the individual command physical security program, and coordinate with the responsible Physical Security Specialist, as required.



JUN 08 2017

(2) Serve as the officer primarily responsible for overseeing the daily implementation of facility physical security measures within the respective AOR, to include the training of other command security personnel.

(3) Perform security system operability functions (e.g., correct installation, operation, calibration, maintenance and testing) at facilities under his/her cognizance, and ensure security personnel receive appropriate training before operating and monitoring security systems and devices.

(4) Create records of physical security system maintenance and testing, and forward them to the responsible Physical Security Specialist.

(5) Maintain records of command training for security personnel and other staff members, and forward such records to the responsible Physical Security Specialist.

(6) In coordination with the responsible Physical Security Specialist, ensure that physical security drills are correctly and routinely performed, and that written after-action reports on such drills are maintained.

(7) Assist RLSO, DSO and NJS COs with the preparation of facility physical security reports and security plans, as required.

(8) Coordinate, as required, with Code 67, CNIC, an OJAG Physical Security Specialist, or NCIS STAAT to ensure completion of an annual security assessment for each NLSC facility within the command.

(9) Report all physical security incidents, violations, vulnerabilities and deficiencies to Director, Code 67, with a copy provided to the responsible Physical Security Specialist, in order to implement appropriate mitigation measures and required investigations.

(10) Coordinate with the cognizant Circuit Military Judge or local judiciary, the cognizant RLSO/DSO/NJS CO, RSO or ISO, CNIC, host installation, and Code 67, as appropriate to implement this program.

k. OJAG Physical Security Officer

(1) Coordinate and administer the OJAG command Physical Security program and execute this instruction.

(2) Coordinate with the host installation and other physical security officers located in or on the same facility and/or installation to implement physical security programs.

(3) Establish a system for the daily after-hours checks of restricted areas, facilities and containers to detect any deficiencies or violations of security standards.

(4) Provide physical security orientation and refresher training to all personnel, as required. Security education programs shall include, but are not limited to, general security safety and awareness, theft prevention, and installation-specific security procedures.

(5) Conduct physical security self-assessments at least annually, and report the results to the Director, Code 67.

(6) Report all physical security incidents, violations, vulnerabilities and deficiencies to Director, Code 67, in order to implement appropriate mitigation measures and required investigations.

(7) Maintain records of program implementation, review and compliance.

(8) Coordinate with the cognizant RSO or ISO, and CNIC, as appropriate, to implement this program.

1. Naval Legal Service Command Inspector General. Review implementation and compliance with this instruction as part of the Article 6 inspection process, and report results as directed by CNLSC.

## 5. Action

### a. Physical Security Requirements

(1) Security requirements under this instruction are categorized as either physical security requirements or risk assessment-specific security requirements. COS-RLSO, COS-DSO, CJDON, AJAG 02, and NLSC COs may promulgate additional security guidelines consistent with this instruction and shall coordinate security procedures and projects with installation commanders and Code 67. Reference (e) shall be consulted when construction or modification of a NLSC courthouse is contemplated. Chapters 3, 4, 5, 6, 11, 12, 14, 15, and 16 of reference (e) are of particular importance and can be located at:  
[http://www.gsa.gov/graphics/pbs/Courts\\_Design\\_Guide\\_07.pdf](http://www.gsa.gov/graphics/pbs/Courts_Design_Guide_07.pdf)

(2) NLSC COs responsible for NLSC facilities without a court facility may request security equipment, identified by this instruction as not required, from AJAG 06, via Code 67. Such request shall include the reasons for the request, an explanation as to why other alternatives do not suffice, and amplifying information on how the equipment will be used.

### (3) Building Access

(a) Visitors to NLSC facilities shall not have uncontrolled direct access to NLSC workspaces and personnel. All NLSC facilities shall be equipped with controlled-access entrances (examples include, but are not limited to, biometric readers, swipe cards, key fobs, and cipher locks) or NLSC staff escorts at points beyond areas designated for the public, unless specifically prohibited by fire code or other similar regulation or order. (Electric strike doors, for example, should not be placed at the entrance to a public waiting room or reception area, but

JUN 08 2017

rather, should be placed, if at all, between the public waiting room or reception area to the individual attorney or paralegal offices). Where resources permit, controlled-access entrances should be used at entry control points (ECPs) where visitors can be identified and may be subject to screening (e.g., bag search and metal detection devices).

(b) NLSC Public ECP. Where practicable, a public ECP shall be designated as the main point of entry to a NLSC command or activity. If a public ECP exists, all persons entering through such public ECP shall, at a minimum, be required to present valid photo identification (e.g., military or dependent identification card, driver's license, Passport, etc.) prior to being granted access to NLSC workspaces and personnel. They may also be screened in accordance with this instruction, to include the use of walk-through metal detectors and/or hand-held metal detectors, and physical inspections of bags and packages.

(c) NLSC Restricted ECP. Assigned NLSC personnel may use controlled-access entrances that are not a part of a public ECP. However, if such personnel choose to enter the NLSC activity through the public ECP, they may be required to present identification and be subjected to regular screening as specified above.

(d) OJAG activities shall follow the security policies and guidance set forth by the respective host installations with respect to building access. If no such guidance exists, OJAG activities should exercise the same physical security posture as NLSC activities with respect to building access and the prevention of visitor uncontrolled direct access to OJAG workspaces and personnel.

(e) The NJS Commanding Officer shall determine appropriate security measures and procedures for building access by visitors and staff, at each NJS location, consistent with the security programs of the respective host installations, and mission requirements.

(4) Placards. Placards shall be prominently displayed at NLSC commands and activities, especially at ECPs, notifying all personnel that they are subject to search at all times. Those not consenting to a search shall not be permitted entry. Placards shall also list prohibited items in accordance with the security plan of the installation at which the facility is located. Individuals found to possess such items while in a NLSC facility may be subject to disciplinary action, removal from the facility, or both. A sample placard is provided in enclosure (3).

(5) Visitor Identification, Log and Escort

(a) All visiting personnel shall present valid photo identification before being granted entry to a NLSC command or activity. Where practicable, visitor badges should be issued to those visitors who are permitted entry. Sample visitor badges are provided in enclosure (4).

(b) A visitor log shall be maintained and kept on file for a period of two years. All visitor log entries and information pertaining to defense, legal assistance and Victims' Legal Counsel clients and services shall be maintained in confidentiality and the information contained therein shall not be released unless such release is required to comply with other valid law, regulation, statute, or court order. A sample visitor log is provided in enclosure (5).

(c) Where RLSO and DSO offices are co-located and share an ECP, a separate log for DSO clients shall be maintained, and viewed, only by DSO personnel.

(d) Local COs shall determine the circumstances under which visitors are and are not required to be escorted, taking into account the missions and functions of the respective offices, as well as the risk assessment of individual military justice proceedings.

#### (6) Duress Alarms

(a) Facilities with a court facility shall be equipped with a duress alarm system capable of notifying base security. Duress alarm activation buttons shall be installed at the judge's bench and in the judge's chambers. Duress alarms shall provide a visual alert to personnel within the facility, and shall also include an audible alarm to augment the visual alarm. Duress alarms should directly alert base security without the need for additional notification after the alarm is activated, and the audio alarm should be supplemented with the capability to verbally alert personnel in the facility of the nature of the alarm and direct personnel movement as necessary. Where duress alarm systems do not directly alert base security, local NLSC security plans shall include procedures to ensure base security is immediately notified of any emergency.

(b) Facilities without a court facility may be equipped with a duress alarm system, with all or any of the features described in the preceding paragraph. If installed, duress alarm activation buttons should be placed at any existing ECP. Where duress alarm systems are not installed or where they do not directly alert base security, local NLSC security plans shall include procedures to ensure base security is immediately notified of any emergency.

(c) All duress alarms shall be tested at least quarterly to ensure connectivity and functionality. Courtroom duress alarms shall be tested at least once the week of any military justice proceeding.

#### (7) Surveillance Systems

(a) Facilities with a court facility shall be equipped with a video surveillance system to monitor internal and external NLSC facility spaces. Placards shall be prominently displayed near external areas notifying personnel that the area is under video surveillance. Surveillance feeds shall be monitored during normal business hours when visitors are present, and especially during military justice proceedings. Because video surveillance is intended to deter, detect and defeat day-to-day security threats in and around the NLSC facility, and is not intended to collect evidence of crime, or create a system of records, the surveillance system is not required to record nor store footage. COs may exercise their discretion to establish local procedures for recording, storing and deleting surveillance footage, consistent with the local system's capabilities. No system shall store footage in excess of two years from the date it was recorded.

(b) Facilities without a court facility may be equipped with a video surveillance system, as described in the preceding paragraph. If installed, placards shall be prominently displayed to notify personnel that the area is under video monitoring surveillance. Surveillance feeds should be monitored during normal business hours when visitors are present.

(8) Metal Detection Devices

(a) Facilities with a court facility shall be equipped with metal detection devices, including either walk-through or handheld detectors. Placement and use of metal detection devices for military justice proceedings shall be in accordance with the risk assessment-specific security requirements below.

(b) Facilities without a court facility may be equipped with metal detection devices, including either walk-through or handheld detectors. If so equipped, metal detectors should be placed at any existing ECP.

(9) Additional Access Controls. Access control systems, activated by biometric readers, cipher locks, swipe cards, proximity cards, or deadbolt locks, shall be installed within NLSC facilities to limit access to sensitive areas, such as judicial chambers, legal assistance and trial/defense counsel offices, and other locations as appropriate, taking into account the unique features of each facility's design or use.

(10) Firearms in NLSC Facilities. The carrying of firearms in a NLSC facility is prohibited, except as noted below or in exigent circumstances.

(a) Per reference (f), NCIS Special Agents are authorized to carry NCIS-approved firearms at all times, while on or off duty, and while on and off installations, aircraft, and ships. NCIS Special Agents are required to carry NCIS-approved firearms while on official business. Accordingly, properly credentialed NCIS Special Agents are permitted access to NLSC spaces while carrying NCIS-approved firearms.

(b) Other (non-NCIS) properly credentialed law enforcement personnel acting in the course of their official duties may be permitted to retain their firearms within NLSC facilities in the discretion of the cognizant CO.

(c) Security personnel qualified and authorized to carry a firearm that are assigned duties supporting a military justice proceeding as part of a security plan are permitted to carry their firearms within the NLSC facility.

(11) Firearms in NLSC Courtrooms. Firearms and other weapons are prohibited within the courtroom during a military justice proceeding unless the presiding military judge (or RLSO CO for Article 32 preliminary hearings) is notified and approves, except in exigent circumstances.

(12) Inspections. All NLSC facilities and spaces shall be inspected for security breaches or compromised access points at the beginning of the day; prior to opening the facility and spaces to visitors, customers, and clients; at any time that the cognizant CO, command physical security officer, or physical security specialist deems necessary; and at the end of the day.

b. Risk Assessment Policy and Procedures

(1) Threat Risk. The threat risk for each military justice proceeding shall be assessed as either “low,” “medium,” or “high,” and shall be mitigated through the use of security measures consistent with this instruction and references (a) through (c). In non-military justice proceedings, NLSC personnel shall exercise sound judgment and take appropriate measures to deter, detect and defeat security threats.

(a) A “low” risk military justice proceeding is a proceeding in which the potential for violence or other types of disruption in and around the court facility is assessed as unlikely. An assessment of low risk does not mean a violent or disruptive act will not occur, but that a violent or disruptive situation is not reasonably anticipated. Participants must still remain vigilant to the possibility of violence or other disruptions during the proceeding.

(b) A “medium” risk military justice proceeding is a proceeding in which the potential for violence or other types of disruption in and around the court facility is assessed as possible and merits the implementation of additional security measures. An assessment of medium risk does not mean that a violent or disruptive act will occur, but that a violent or disruptive act might be expected.

(c) A “high” risk military justice proceeding is a proceeding in which the potential for violence or other types of disruption in and around the courthouse is assessed as reasonably foreseeable and merits additional security measures. An assessment of high risk does not mean a violent or disruptive act will occur, but that a violent or disruptive act could reasonably be expected to occur.

(2) Risk Assessment Procedures

(a) RLSO COs and AJAG 02 shall ensure that an initial risk assessment of every military justice proceeding is completed and provided to participating personnel (e.g., the cognizant Circuit Military Judge, appellate judge, or detailed military trial judge, and convening authority) not later than 72 hours before the initial military justice proceeding in a case. Enclosure (2), which is available as a “fillable” .pdf, is provided as a tool to assist in conducting risk assessments and may be modified to suit the particular needs of the command and/or the proceeding.

(b) When participating in military justice proceedings involving DSO personnel but not RLSO personnel, DSO COs shall ensure that an initial risk assessment is completed, as above, in coordination with a physical security specialist, local security personnel, and other interested parties, not later than 72 hours before the initial military justice proceeding.

(c) COs shall notify AJAG 06, via Code 67 of proceedings assessed as “medium” risk 72 hours before the initial military justice proceeding in each case, to the maximum extent practicable. Likewise, COs shall notify AJAG 06, via Code 67, as soon as practicable, when a subsequent military justice proceeding, initially assessed as “low” risk, is later reassessed as “medium” or “high” risk.



(d) Reports of military justice proceedings assessed as "medium" or "high" risk shall be forwarded to the cognizant NCIS SAC and/or ISO, for their awareness and coordination for any required support.

(3) Risk Assessment Factors. NLSC personnel should consider any and all elements in assessing the risk level of a case, in addition to those criteria listed below. The following factors are meant to serve as a guide in evaluating the relative risk associated with a particular military justice proceeding. No one factor is more important than another and this is not an exhaustive list:

- (a) the nature of the underlying allegation(s) associated with the proceeding;
- (b) the presence of the accused, victim, witnesses, and family members at the proceeding;
- (c) the mental, physical, and criminal history, if known, of the accused, victim, witnesses, family members, or other parties with a direct or indirect interest in the proceedings;
- (d) the accused's CO's overall assessment of risk to personnel or facilities;
- (e) the level of expected media interest;
- (f) the level of expected community impact or interest; and
- (g) any other facts or circumstances known to NLSC personnel that would assist in assessing the relative risk associated with the military justice proceeding.

(4) All subsequent military justice proceedings in a particular case will assume the same risk assessment as the initial risk assessment. However, if new or additional information becomes available at any point during the military justice proceedings that causes NLSC or law enforcement personnel to believe the initial risk assessment of the military justice proceeding no longer adequately reflects the perceived threat to personnel and physical security, the responsible CO shall ensure a new risk assessment is conducted.

c. Risk Assessment-Specific Court Facility Security Requirements

(1) "High" and "Medium" Risk Military Justice Proceedings. The following security guidelines shall be applicable during the conduct of "high" and "medium" risk military justice proceedings, or as otherwise required by the cognizant CO.

(a) "High" Risk Security Plans. The cognizant CO shall submit a written security plan that identifies potential threats, security vulnerabilities, and mitigating efforts, for approval, to AJAG 06 via Code 67 (copying the circuit judge, COS-DSO, military judge, RLSO or DSO CO as appropriate, and all interested counsel and security personnel) not later than 72 hours prior to the initial military justice proceeding in a case. Likewise, the cognizant CO shall submit a written security plan, as soon as practicable, when a subsequent military justice proceeding,

JUN 08 2017

initially assessed as "low" or "medium" risk, is later reassessed to be "high" risk. AJAG 06 will respond in writing, either approving or disapproving the security plan.

(b) Courtroom Security

1. "High" Risk. At least two Naval Security Force (NSF) personnel shall be present in the NLSC facility for "high" risk military justice proceedings. The CO shall consult with the respective RSO/ISO and NCIS SAC for assistance as appropriate, in accordance with reference (c). The NSF personnel shall be posted in locations that allow for their immediate response to threats and disturbances inside the courtroom.

2. "Medium" Risk. At least one NSF member shall be present in the NLSC facility for "medium" risk military justice proceedings. The CO shall consult with the respective RSO/ISO and NCIS SAC for assistance as appropriate, in accordance with reference (c). The NSF member shall be posted in a location that allows for his or her immediate response to threats and disturbances inside the courtroom.

(c) Access Controls and Metal Detection

1. Public ECP. If not already established as a part of the minimum physical security requirements for NLSC facilities pursuant to paragraph 5a(3)(a) above, a public ECP, equipped with functioning walk-through or handheld metal detectors, shall be designated as the main point of entry to the NLSC facility containing the courtroom, for "high" and "medium" risk proceedings. All persons, with the exception of NLSC/OJAG personnel who are assigned to the facility and identified law enforcement personnel, shall be screened in accordance with this instruction. The cognizant CO may approve screening exceptions for other individuals, but must do so in writing and provide a copy of such written exceptions to ECP security personnel. The public ECP shall be staffed by a minimum of two appropriately trained personnel. Personnel assigned to staff the public ECP shall not be tasked with any other duties while manning the ECP. The public ECP should be positioned at the main entrance of the building and allow for the smooth flow of foot traffic through the metal detection area and, where practicable, should not provide a direct line of sight into court facilities, witness waiting rooms, or trial counsel/defense counsel offices.

2. Secondary Screening. A secondary ECP shall be situated close to entry into the courtroom and shall be equipped with either a walk-through or hand-held metal detection device. All persons, with the exception of exempted personnel, entering the courtroom through the public ECP shall be rescreened prior to entering the courtroom. The secondary screening ECP should be positioned to allow for the smooth flow of foot traffic through the secondary metal detection area and should not have a direct line of sight into the courtroom, adjacent witness waiting rooms, or trial counsel/defense counsel offices.

3. Visitor Identification. All visiting personnel shall present valid photo identification before being granted entry to the courtroom, and shall be issued a visitor badge, if one was not previously issued. Visitor badges shall be prominently displayed by visitors at all times. A visitor log shall be maintained at the public ECP and kept on file for a period of two years. All

JUN 08 2017

visitor logs shall be maintained in confidentiality and the information contained therein shall not be released unless such release is required to comply with other valid law, regulation, statute, or court order. Local COs shall determine the circumstances under which visitors are and are not required to be escorted, taking into account the risk assessment of individual military justice proceedings. Sample visitor logs and visitor badges are provided in enclosures (4) and (5).

(d) Inspections. In addition to the inspections conducted at the beginning and the end of the day at all NLSC facilities, courtrooms shall be inspected for security breaches or compromised access points prior to opening the facility and spaces to visitors, customers, and clients; after all breaks of the military justice proceedings (e.g., lunch or extended recess); or at any time that the cognizant CO, command physical security officer, or physical security specialist deems necessary. The command physical security officer shall assign personnel to perform these courtroom inspections.

(2) "Low" Risk Military Justice Proceedings. The following security guidelines shall be applicable during the conduct of "low" risk military justice proceedings, or as otherwise required by the cognizant CO.

(a) Access Controls. There shall be at least one screening point entrance to the courtroom, equipped with metal detection devices. All persons, with the exception of exempted personnel, entering the courtroom through this entrance shall be screened prior to entering the courtroom. The ECP to the courtroom should be positioned to allow for the smooth flow of foot traffic through the metal detection area and should not have a direct line of sight into the courtroom, adjacent witness waiting rooms, or trial counsel/defense counsel offices. If visitor screening and metal detection is performed at the main ECP to the facility, a second screening area for access to the courtroom is not required.

(b) Metal Detection Devices. Walk-through or hand-held metal detectors shall be used to screen all personnel, with the exception of NLSC/OJAG personnel and identified law enforcement personnel, prior to entering the courtroom through the courtroom ECP.

(c) Inspections. In addition to the inspections conducted at the beginning and the end of the day at all NLSC facilities, courtrooms shall be inspected for security breaches or compromised access points prior to opening the facility and spaces to visitors, customers, and clients; after all breaks of the military justice proceedings (e.g., lunch or extended recess); or at any time that the cognizant CO, command physical security officer, or physical security specialist deems necessary. The command physical security officer shall assign personnel to perform these courtroom inspections.

## 6. Procedures

### a. Local Assessments

(1) Drills. The command physical security officer or physical security specialist shall conduct periodic notice and no-notice drills to test command security procedures and equipment, and to ensure all hands know their respective roles in the case of a security emergency.

JUN 08 2017

Approval from the respective NLSC CO and coordination with other NLSC personnel are required when conducting drills, especially when conducting no-notice drills. At a minimum, the command security officer or physical security specialist shall conduct one security drill per quarter for each NLSC facility within their respective AORs. Drills will be as realistic as possible; however, safety is of paramount concern, and appropriate safety controls will be in place at all times during all drills.

(2) After-Action Reports (AAR). The command physical security officer or physical security specialist shall document and maintain results of drills through AARs. AARs shall be submitted to the responsible CO for his/her review. AARs are subject to review as part of the Article 6 inspection process and shall be maintained at least until the next Article 6 inspection.

b. Reporting Requirements. COs shall provide quarterly security reports to AJAG 06, via Code 67 (copying the local military judge, respective RLSD/DSO CO, and respective Physical Security Specialist) for all facilities under their cognizance. The report should include the status of all security equipment, AARs of drills conducted during the time period covered, plans for security drill(s) for the next quarter, details on physical security training completed, and any facility or security requirement deficiencies. A sample quarterly security report is provided in enclosure (6).

c. Waivers. Where resources or facility limitations prevent compliance with this instruction or where situations not contemplated by this instruction arise, the cognizant CO shall request a waiver, in writing, from AJAG 06, via Code 67, if the CO deems operations should continue despite the deficiency. A copy of all waiver requests shall be sent to the cognizant Physical Security Specialist assigned responsibility for the command. Waiver requests shall describe the deficiency, explain the command's efforts to develop a suitable alternative solution to mitigate risk, delineate a plan to correct the deficiency, and provide a projected completion date to correct the deficiency. Code 67 shall act upon waiver requests, within 72 hours of submission, by making a recommendation to AJAG 06. AJAG 06 will respond in writing, either approving or disapproving the request. A sample waiver request is provided in enclosure (7).

7. Questions or concerns regarding this instruction should be addressed to Deputy Division Director for Operations, Code 67 via the Code 67 SharePoint portal for Physical Security, located at:

<https://portal.secnave.navy.mil/orgs/JAG/67/operations/SitePages/PhysicalSecurity.aspx>. All physical security documents are available on the Physical Security SharePoint portal.

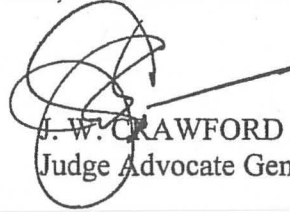
8. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 of January 2012.

9. Review and Effective Date. Code 67 will review this instruction annually on the anniversary of the effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority, using OPNAV 5215/40 Review of

Instruction. This instruction will automatically expire 5 years after effective date unless reissued or otherwise canceled prior to the 5-year anniversary date, or an extension has been granted.



JOHN G. HANNINK  
Commander, Naval Legal Service Command



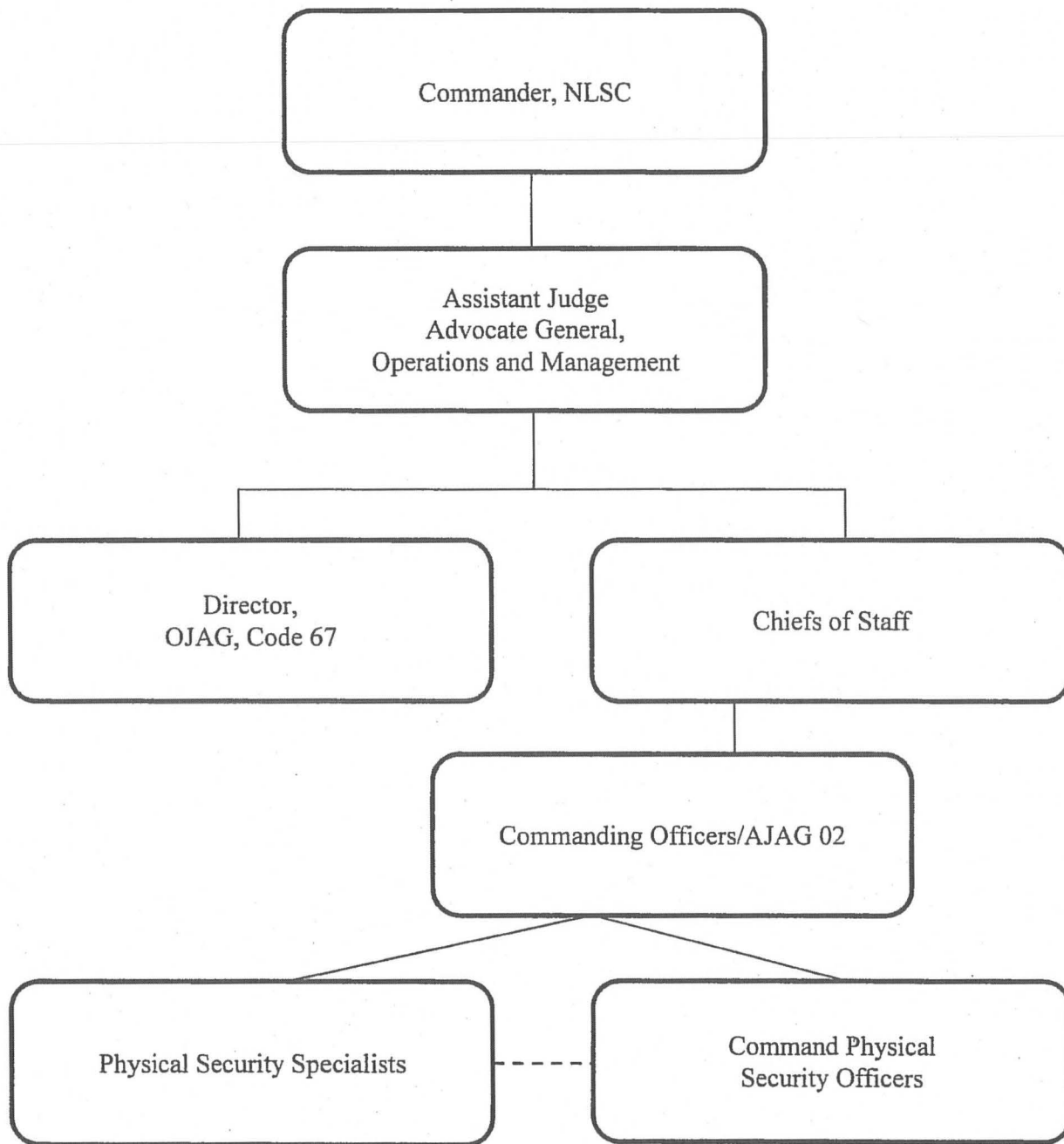
J. W. CRAWFORD III  
Judge Advocate General

---

Releasability and Distribution:

This instruction is cleared for public release and is available electronically only via the OJAG Website  
<http://www.jag.navy.mil>

OJAG PHYSICAL SECURITY ORGANIZATIONAL CHART



Reflects relationships and authorities only for purposes of physical security management under this instruction and does not reflect established command relationships under the SOM. Chief of Staff will adjudicate any potential conflict that may arise in the execution or management of PSS and their duties.



JUN 08 2017

MILITARY JUSTICE PROCEEDING  
RISK ASSESSMENT INSTRUCTIONS

This document shall be used when conducting initial risk assessments and reassessments of military justice proceedings, in accordance with JAG/CNLSCINST 5530.2D. The initial risk assessment of a case shall apply to all subsequent military justice proceedings in that same case, unless new or additional information becomes available and requires a reassessment of the relative risk. Specific instructions for completion of this document follow; however, additional notifications and reports may be required by JAG/CNLSCINST 5530.2D. Unless otherwise indicated in these instructions in bold, any person involved in the proceeding may provide information to complete required fields.

**CAVEAT:** The form allows for electronic signature. The use of a physical signature will lose the form's ability for subsequent electronic signatures or further electronic entry.

The three risk assessment levels are:

**Low risk proceeding** - a proceeding in which the potential for violence or other types of disruption in and around the courthouse is assessed as unlikely. An assessment of low risk does not mean a violent or disruptive act will not occur, but that a violent or disruptive situation is not reasonably anticipated.

**Medium risk proceeding** - a proceeding in which the potential for violence or other types of disruption in and around the courthouse is assessed as possible and merits the implementation of additional security measures. An assessment of medium risk does not mean that a violent or disruptive act will occur, but that a violent or disruptive act might be expected.

**High risk proceeding** - a proceeding in which the potential for violence or other types of disruption in and around the courthouse is assessed as reasonably foreseeable and merits additional security measures. An assessment of high risk does not mean a violent or disruptive act will occur, but that a violent or disruptive act could reasonably be expected.

Enter the case name, then select the type of proceeding from the dropdown menu. Enter the date of the proceeding. Enter the facility location in which the proceeding will take place, the charges associated with the proceeding, and the Accused's total years of service.

Collect input in no particular order from the interested parties about information relevant to the risk assessment. These parties include the Convening Authority (CA), Accused's Commanding Officer (CO), Trial Counsel (TC), Defense Counsel (DC), and Victim Legal Counsel (VLC). Check the "NO INPUT" box in their section if no information is provided. If the Accused's CO is also the Convening Authority, check the "CO IS CA" box under CO section. If the case does not have a VLC, check the "N/A" box under VLC section. The individual responsible for gathering this information will electronically sign at the bottom of the first page to indicate all parties were notified, were provided an opportunity to respond, and have their input accurately reflected on the assessment. The individual gathering this information should keep a record of each party's input or note on the form as to how the information was acquired.

Enclosure (2)

MILITARY JUSTICE PROCEEDING  
RISK ASSESSMENT INSTRUCTIONS

If the proceeding will take place in a NLSC facility or in a Non-NLSC facility that involves Region Legal Service Office (RLSO) personnel, the final risk assessment shall be completed by the **RLSO CO**. He/she shall use the dropdown menu to indicate the risk assessment level, and also either digitally or physically sign and date the document. He/she may use the text field to notate other facts or circumstances that were used in the assessment.

If the proceeding will take place in a non-NLSC facility that involves only Defense Service Office (DSO) personnel, the final risk assessment shall be completed by the **DSO CO** who is responsible for the physical security of the DSO personnel involved in the proceeding. He/she shall use the dropdown menu to indicate the risk assessment level, and also either digitally or physically sign and date the document. He/she may use the text field to notate other facts or circumstances that were used in the assessment.

For cases assessed as Medium or High Risk by the CO, route the assessment to NCIS for their review and acknowledgement. NCIS shall then either digitally or physically sign and date the document. Check "N/A" for Low Risk cases when the acknowledgement is not required.

Should proceedings in a case continue and a military judge (MJ) is later assigned, route this document to the MJ for their review and acknowledgement. The MJ shall then either digitally or physically sign and date the document.

The completed document shall then be routed in accordance with JAG/CNLSCINST 5530.2D.

If a reassessment is required, select the previous risk level from the dropdown box. Enter the date of that assessment. Enter the facts and circumstances explaining the need for a reassessment. The appropriate CO shall then use the dropdown menu to indicate the updated risk assessment level, and also either digitally or physically sign and date the document.

All parties are advised to consider the relevance, necessity, propensity for objection, and privacy concerns of all information provided for, and included on, this document.

**MILITARY JUSTICE PROCEEDING – RISK ASSESSMENT**United States v. Proceeding: Date: Location: Charges: Accused's Years of Service: 

Provide input on any concerns, threats, vulnerabilities, or issues related to the potential for violence or other types of disruption in and around the court facility. Among other relevant interests, include information about the parties expected to be present at the proceeding; any known mental, physical, or criminal history of the Accused or any party expected to be at the proceeding; and the level of media interest.

CA:

NO INPUT

☐

Accused's CO:

NO INPUT

☐

CO IS CA

☐

TC:

NO INPUT

☐

*NOTE: DC and VLC are not requested to provide privileged information; however, they should relay any non-privileged information they are reasonably aware of that may help inform RLSO/DSO CO in making a risk determination.*

DC:

NO INPUT

☐

VLC:

NO INPUT

☐

N/A

☐

All of the above parties were consulted and provided an opportunity to advise on the risk level of the referenced proceeding. Their input is accurately and completely included in this form.

FOR OFFICIAL USE ONLY

**FINAL RISK ASSESSMENT:**

*Any additional facts or circumstances known to the CO, and used in making the risk assessment.*

RLSO CO / DSO CO

N/A  
☐

REVIEW & ACKNOWLEDGEMENT OF NCIS  
*(For MEDIUM and HIGH Risk cases only)*

REVIEW & ACKNOWLEDGEMENT OF MJ

**UPDATE ONLY:** If new information creates the need for reassessment, document the change in risk level below.

**Previous Risk:**

**Completed:**

**New information:**

**UPDATED RISK ASSESSMENT:**

RLSO CO / DSO CO

# WARNING



YOU ARE NOW ENTERING A FEDERAL FACILITY. ENTRY CONSTITUTES CONSENT TO SEARCH YOUR PERSON AND THE PROPERTY UNDER YOUR CONTROL. REFUSAL TO CONSENT TO SEARCH WILL RESULT IN ENTRY TO THE FACILITY BEING DENIED. (INTERNAL SECURITY ACT OF 1950, 50 U.S.C. § 797)

---

**THE FOLLOWING ITEMS ARE PROHIBITED IN THIS FACILITY:**

**FIREARMS  
KNIVES  
DANGEROUS WEAPONS  
CELL PHONES  
CAMERAS  
ELECTRONIC DEVICES  
OTHER ITEMS PROHIBITED BY THE UNIFORM CODE  
OF MILITARY JUSTICE, FEDERAL OR STATE LAW  
(18 U.S.C. § 930 AND APPLICABLE U.S. NAVY POLICY)**

POSSESSION OF SUCH ITEMS WILL RESULT IN SEIZURE OF THE ITEM, DENIAL OF ENTRY TO THE FACILITY, AND POSSIBLE LEGAL AND/OR DISCIPLINARY ACTION. BAGS, PURSES AND BACKPACKS MAY BE PROHIBITED WHEN DEEMED NECESSARY BY THE COMMANDING OFFICER.

---

**ALL PERSONNEL IN THIS AREA ARE UNDER VIDEO MONITORING SURVEILLANCE.**

Enclosure (3)

## [COMMAND, FACILITY] VISITOR LOG

## DATE \_\_\_\_\_

[illegible]



**VISITOR**

**NO escort  
required**

**Badge #1**

**VISITOR**

**YES escort  
required**

**Badge #1**

**VISITOR**

**NO escort  
required**

**Badge #2**

**VISITOR**

**YES escort  
required**

**Badge #2**

JAG/COMNAVLEGSVCCOMINST 5530.2D

From: Commanding Officer, (insert command)  
To: Assistant Judge Advocate General-Operations and Management  
Via: Office of the Judge Advocate General, Code 67

Subj: QUARTERLY PHYSICAL SECURITY REPORT FOR (#) QUARTER FY(##)

---

Ref: (a) JAG/COMNAVLEGSVCCOMINST 5530.2D

Encl: (1) Security Equipment Report  
(2) Alarm Test Report  
(3) Security Drill After Action Report(s)  
(4) Physical Security Committee Meeting Minutes (as applicable)

1. In accordance with reference (a), the following physical security information is provided:

- a. Operating status of physical security equipment/alarms  
(provide summary)
- b. Physical security drill(s) conducted  
(provide details/results)
- c. Physical security drills planned for next quarter  
(provide details)
- d. Physical security incidents/deficiencies/issues  
(provide summary)
- e. Training completed  
(provide summary)

2. Other amplifying information.

3. Point of contact for physical security matters is (insert name and contact information).

SIGNATURE

Copy to:  
Circuit Military Judge  
Local DSO/RLSO CO, as appropriate

Enclosure (6)

**ALARM TEST REPORT**

<b>Reporting Command:</b>		<b>Facility Location:</b>	<b>Date of Submission:</b>	<b>Command POC:</b>
(Command Name)		(Branch Office/Det/Etc.)	(Date)	(Name)
<b>Nature of Alarm Test</b>	<b>Date/Time of Test</b>	<b>Location</b>	<b>Results</b>	<b>Comments</b>
(e.g., Silent, No-notice, Notice)		(e.g., Courtroom #1, Judge's Bench)	(e.g., Fully Operational)	(e.g., None or Need to Adjust Volume)

**Command Name**  
**Physical Security Quarterly Report**  
**# Quarter FY##**

JAG/COMNAVLEGSVCCOMINST 5530.2D

<b><u>SECURITY EQUIPMENT REPORT</u></b>				
<b>Reporting Command:</b>		<b>Facility Location:</b>	<b>Date of Submission:</b>	<b>Command POC:</b>
(Command Name)		(Branch Office/Det/Etc.)	(Date)	(Name)
<b>Equipment Description</b>	<b>Qty</b>	<b>Physical Location</b>	<b>Operating Status</b>	<b>Comments/Deficiencies</b>
(e.g., Handheld Metal Detector)	#	(e.g., Installation, Building, Room)	(e.g., Fully Operational)	(e.g., None or Repair Needed)

JAG/COMNAVLEGSVCCOMINST 5530.2D

Ser

Date

From: Commanding Officer, (insert command)  
To: Assistant Judge Advocate General-Operations and Management  
Via: Office of the Judge Advocate General, Code 67

---

Subj: REQUEST FOR WAIVER FROM PHYSICAL SECURITY PROGRAM  
REQUIREMENT DUE TO (insert description)

Ref: (a) JAG/COMNAVLEGSVCCOMINST 5530.2D

Encl: (1) As Appropriate  
(2) As Appropriate

1. In accordance with reference (a), I respectfully request a waiver from the physical security program requirement to (insert description).
2. Explain requirement and how it is not met.
3. Explain the command's efforts to develop a suitable alternative solution to mitigate risk.
4. Explain how the command plans to correct the deficiency, including the projected completion date of the correction.
5. Other amplifying information.
6. Point of contact for this physical security waiver request is (insert name and contact information).

SIGNATURE

Enclosure (7)