

UNCLASSIFIED




United States Cyber Command Instruction (USCCI)

OPR: J006
EDITION: A

USCCI 2305-01
DEC 21 2020

Law of War Program

1. Purpose. This instruction implements the Department of Defense (DOD) Law of War Program within United States Cyber Command (USCYBERCOM).
2. Supersedes/Cancellation. This is the first issuance.
3. Applicability. This instruction applies to all United States (U.S.) Armed Forces personnel, including civilians and civilian DOD contractors, assigned or attached to USCYBERCOM, the Cyber National Mission Force (CNMF), Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN), Joint Force Headquarters-Cyberspace (JFHQ-C), Service Component Commands (SCC), and joint task forces (JTF). This USCCI is applicable at all times and applies to all military operations and activities.
4. Policies. Policies are outlined in each enclosure and in the references in Attachment 1.
5. Releasability. Cleared for Public Release. This instruction is approved for public release; distribution is unlimited. DOD Components, other federal agencies, and the public may obtain copies of this instruction.
6. Effective Date. This instruction is effective upon signature.


DAVID T. ISAACSON
Major General, U.S. Army
Chief of Staff

Enclosures:

- Enclosure 1 – Policy
- Enclosure 2 – Roles and Responsibilities
- Enclosure 3 – Reporting and Investigation Processes
- Attachment 1 – Glossary of References and Supporting Information

UNCLASSIFIED

ENCLOSURE 1

1. Policy. USCYBERCOM, CNMF, JFHQ-DODIN, the JFHQ-Cs, the SCCs, and JTFs ensure compliance with the law of war during armed conflict, however characterized. In military operations, USCYBERCOM acts consistent with the law of war's fundamental principles and rules, which include those in Common Article 3 of the 1949 Geneva Conventions and the principles of military necessity, humanity, distinction, proportionality, and honor. Specifically, USCYBERCOM policy addresses the following.

1.1. Applicability of the Law of War to Cyberspace Operations (CO). Precisely how the law of war applies to CO is not well settled, and aspects of the law in this area are likely to continue to develop, especially as new cyberspace capabilities are developed and States determine their views in response to such developments. Specific law of war rules may apply to CO, even though those rules were developed before CO were possible. Applicability of specific rules turns on whether a proposed CO constitutes an attack, or an act of violence, under *jus in bello*. For example, CO that do not constitute an attack are not strictly bound by targeting principles. When no more specific law of war rule or other applicable rule applies, law of war principles provide a general guide for conduct during CO.

1.2. Observation and Enforcement. The law of war and the obligations of the U.S. Government are observed and enforced by USCYBERCOM, CNMF, JFHQ-DODIN, the JFHQ-Cs, the SCCs, JTFs, and DOD contractors or subcontractors assigned to or accompanying U.S. Armed Forces.

1.2.1. All military and U.S. civilian employees, contractor personnel, and subcontractors assigned to or accompanying a DOD Component shall report all reportable incidents through their chain of command and servicing judge advocates or legal advisors, including those involving allegations of non-DOD personnel having violated the law of war.

1.2.2. Such reports may also be made through other channels such as the military police, a judge advocate, or an Inspector General (IG). Reports made to officials other than those specified in this paragraph shall, nonetheless, be accepted and immediately forwarded through the recipient's chain of command and servicing judge advocates or legal advisors.

1.3. Program. An effective program designed to prevent violations of the law of war is implemented by USCYBERCOM, CNMF, JFHQ-DODIN, the JFHQ-Cs, the SCCs, and JTFs. The program consists of:

1.3.1. Law of war dissemination and periodic training on the law of war.

1.3.2. Legal advisers advising on the law of war and military operations.

1.3.3. Procedures to implement law of war standards and establish processes for ensuring compliance.

1.3.4. Reporting mechanisms for incidents to ensure that commanders can exercise their responsibilities to implement and enforce the law of war. Promptly report all reportable incidents, as defined in this instruction, through the chain of command in accordance with (IAW) the requirements of Enclosure 3.

1.3.5. Assessments, investigations, inquiries, or other reviews of incidents needed to determine appropriate responses, which may include:

1.3.5.1. Additional review or investigation, such as referral to the respective Service criminal investigative organization or IG's office.

1.3.5.2. Transmission to relevant U.S. departments and agencies, partner governments, or other authorities with responsibilities with respect to the reportable incident.

1.3.5.3. Accountability or improvement actions.

1.3.6. Appropriate actions to ensure accountability and to improve efforts to prevent violations of the law of war in U.S. military operations. Such actions may include:

1.3.6.1. Providing additional training.

1.3.6.2. Taking adverse or corrective administrative action, including non-judicial punishment.

1.3.6.3. Instituting criminal proceedings.

1.3.6.4. Revising or issuing policies, regulations, instructions, procedures, training documents, or other guidance to incorporate lessons learned.

1.4. Acquisition and Procurement. The intended acquisition, procurement, or modification of cyberspace capabilities for use as a weapon or weapon system is reviewed for consistency with the law of war by the USCYBERCOM Staff Judge Advocate (J006 [SJA]).

ENCLOSURE 2

2. Roles and Responsibilities.

2.1. **General.** USCYBERCOM, CNMF, JFHQ-DODIN, the JFHQ-Cs, the SCCs, and JTFs will:

2.1.1. Comply with the policies and processes contained in this instruction.

2.1.2. Incorporate qualified legal advisers into training and advising on the law of war and military operations.

2.1.3. Promulgate the policies and procedures to implement law of war standards into plans, operations, and training programs and establish processes for ensuring compliance, particularly in light of any reported violations.

2.1.4. Comply with reporting mechanisms for suspected reportable incidents to ensure that commanders can exercise their responsibilities to implement and enforce the law of war. Promptly report all suspected reportable incidents, as defined in this instruction, through the chain of command and servicing judge advocates IAW the requirements of Enclosure 3.

2.1.5. Conduct and report assessments, investigations, inquiries, or other reviews of suspected reportable incidents needed to determine appropriate responses through the chain of command and servicing judge advocates or legal advisors IAW the requirements of Enclosure 3.

2.1.6. Conduct appropriate actions to ensure accountability and to improve efforts to prevent violations of the law of war in U.S. military operations, to include providing effective training regarding the principles and rules of armed conflict commensurate with a member's duties and responsibilities. Exercises and training will include law of war scenarios or items to improve evaluation, responses, and reporting procedures.

2.1.7. Where applicable, coordinate for a weapon or weapon system legal review where the intended acquisition, procurement, or modification of cyberspace capabilities is intended for use as a weapon or weapon system.

2.1.8. Ensure that contract work statements for contractors and their subordinates comply with the policies contained in this instruction, DOD Directive (DODD) 2311.01, *DOD Law of War Program*, and DOD Instruction (DODI) 3020.31, *Operational Contract Support (OCS)*. Contracts should require contractors to implement effective programs to prevent violations of the law of war by their employees and subcontractors, including programs for law of war dissemination and periodic training commensurate with each individual's duties and responsibilities.

2.1.9. In addition to reporting a Law of War incident to the Director of Operations (J3), report a violation that qualifies as a Significant or Highly Sensitive Matter (S/HSM) to the USCYBERCOM Intelligence Oversight Program Management (IOPM) Office for processing IAW DOD Directive (DODD) 5148.13, *Intelligence Oversight*.

2.2. Chief of Staff (CoS).

2.2.1. Maintains records of suspected reportable incidents, to include USCYBERCOM's central collection of reportable incidents IAW the requirements of Enclosure 3.

2.2.2. Submits completed investigations and inquiries to the Chairman of the Joint Chiefs of Staff (CJCS), the Secretary of Defense (SecDef), the Commander, United States Special Operations Command (CDRUSSOCOM), if applicable, and relevant Secretaries of the Military Departments.

2.3. Director of Intelligence (J2). Assists gathering relevant information on suspected reportable incidents.

2.4. Director of Operations (J3).

2.4.1. Submits reportable incidents through Commander, USCYBERCOM (CDRUSCYBERCOM) to the CJCS, the SecDef, the CDRUSSOCOM, if applicable, and relevant Secretaries of the Military Departments.

2.4.2. In coordination with (ICW) the Director of Exercises and Training (J7) and J006, identifies law of war-related tasks and knowledge, skills and abilities (KSA) for incorporation into training and certification standards for assigned or attached personnel tasked to conduct or support CO.

2.4.3. Joint Operations Center (JOC).

2.4.3.1. Establishes and ensures reporting mechanisms to capture and account for suspected reportable incidents.

2.4.3.2. Ensures suspected reportable incidents are assessed and processed IAW the requirements of Enclosure 3.

2.4.3.3. Supports CoS maintenance of USCYBERCOM's central collection of reportable incidents.

2.5. Director of Plans and Policy (J5). ICW J006, ensures USCYBERCOM plans remain compliant with the law of war during the biennial reviews of USCYBERCOM plans.

2.6. Director of Exercises and Training (J7).

2.6.1. ICW the J3 and J006, ensures the appropriate exercises include law of war scenarios to improve evaluation, response, and reporting procedures, and that commanders include these scenarios in appropriate exercise events.

2.6.2. ICW the J3 and J006, incorporates law of war-related tasks and KSAs into training and certification standards for assigned or attached personnel tasked to conduct or support CO.

2.7. Staff Judge Advocate (J006).

2.7.1. ICW J7, establishes a law of war training program.

2.7.2. Advises on suspected reportable incidents and investigations.

2.7.3. Ensures cyberspace capabilities intended for use as a weapon or weapon system are reviewed for compliance IAW with DODD 5000.01, *The Defense Acquisition System*; DODD 3000.03E, *DOD Executive Agent for Non-Lethal Weapons (NLW)*, and *NLW Policy*, and DODD 3000.09, *Autonomy in Weapons Systems*, as applicable.

2.8. Public Affairs Office (PAO).

2.8.1. Answers media queries and provides public affairs guidance to the Directorates (if an incident is of interest to the media).

2.8.2. Drafts, ICW Legislative Liaison (LL) and J006, remarks for CDRUSCYBERCOM (or other USCYBERCOM senior leader) to respond to incident inquiries.

2.9. **Legislative Liaison (LL).** Supports Congressional inquiry responses on suspected incidents and investigations.

2.10. **The Inspector General (IG).**

2.10.1. Conducts command inspections and audits to ensure compliance with the public law, governing regulations, policies, and standards concerning compliance with the law of war.

2.10.2. Conducts investigations into allegations of reprisal, abuse of authority or other areas as directed by the CDRUSCYBERCOM, concerning compliance with the law of war.

ENCLOSURE 3

3. Reporting and Investigation Processes.

3.1. **General.** All reportable incidents are reported through command channels to USCYBERCOM J3 for further transmission to appropriate U.S. agencies, partner governments, or other appropriate authorities. Incidents qualifying as S/HSM are also reported through the USCYBERCOM IOPM.

3.1.1. USCYBERCOM, CNMF, JFHQ-DODIN, the JFHQ-Cs, the SCCs, and JTFs provide for the central collection of reports and investigations of reportable incidents alleged to have been committed by or against members of the command or persons accompanying them. CNMF, JFHQ-DODIN, the JFHQ-Cs, the SCCs, and JTFs will forward these reports through the appropriate service components to USCYBERCOM J3 and J006 for further forwarding to the CJCS, SecDef, CDRUSSOCOM, if applicable, and relevant Secretaries of the Military Departments.

3.1.2. No later than (NLT) 31 March and 30 September of each year, USCYBERCOM will update their central collection of reports and investigations and ensure accessibility by SecDef. The central collection includes:

3.1.2.1. The reportable incidents reported to SecDef in the previous six months.

3.1.2.2. The disposition, if any, of each reportable incident within USCYBERCOM.

3.1.2.3. The results of any review or investigation of reportable incidents completed within USCYBERCOM in the previous six months and any such information forwarded by the Military Departments.

3.1.2.4. Information on any significant corrective actions taken within USCYBERCOM and any such information forwarded by the Military Departments.

3.1.2.5. Any additional information CDRUSCYBERCOM deems relevant and appropriate to include, such as determinations that an allegation was not supported by credible information.

3.2. Reporting Law of War Allegations.

3.2.1. **Duty to Report Incidents.** All military and U.S. civilian employees, contractor personnel, and subcontractors assigned to or accompanying a DOD Component shall report all reportable incidents through their chain of command and servicing judge advocates or legal advisors, including those involving allegations of non-DOD personnel having violated the law of war.

3.2.1.1. Such reports may also be made through other channels such as the military police, a judge advocate, or an IG. Reports made to officials other than those specified in this paragraph shall, nonetheless, be accepted and immediately forwarded through the recipient's chain of command and servicing judge advocates or legal advisors. Forward these reports to the chain of command and servicing judge advocates or legal advisors of the subject of the allegation, where appropriate.

3.2.1.2. Contracts must require contractor employees to report reportable incidents to the commander and servicing judge advocate or legal advisor of the unit they are accompanying or supporting or the installation to which they are assigned, or to the appropriate Combatant

Commander. Review and update contracts to ensure compliance with the requirement to report reportable incidents IAW DODD 2311.01.

3.2.2. Receipt of Suspected Incident. Upon receipt of a suspected reportable incident, supervisors will immediately notify the chain of command (including service element), director of the member concerned, and their servicing judge advocate.

3.2.2.1. The commander or task force leader of any unit or organization that obtains information about an alleged law of war violation assesses whether the allegation is based on credible information, and thus constitutes a reportable incident. If the commander or task force leader determines that an allegation is not supported by credible information, the allegation nonetheless forward the allegation through the chain of command and servicing judge advocates to CDRUSCYBERCOM with this determination.

3.2.2.2. Subject to operational constraints, the on-scene commanders or task force leaders take appropriate measures to preserve on-scene evidence of reportable incidents pending transfer to U.S., allied, or other appropriate authorities.

3.2.2.3. If the commander or task force leader determines U.S. persons are not involved in a reportable incident, continue a U.S. investigation or review only at the direction of CDRUSCYBERCOM. Such incidents must still be reported to ensure compliance with the requirements of 10 U.S.C. § 362 and associated DOD policies regarding providing assistance to units of foreign security forces that have committed gross violations of human rights (commonly referred to as Leahy Vetting).

3.2.3. Initial Report. The commander or task force leader of any unit or organization that obtains information about a reportable incident shall immediately report the incident through command and servicing judge advocate or legal advisor channels to the CDRUSCYBERCOM. The report is made through the most expeditious means available, but NLT 12 hours after obtaining information about a reportable incident. To the extent possible, the report includes the following (but not limited to):

3.2.3.1. Who made the allegation and other potential witnesses?

3.2.3.2. Who allegedly participated in the alleged incident, to include whether the alleged participant is associated with another U.S. agency or private cybersecurity partner or foreign partner and whether USCYBERCOM received advance deconfliction or notice of the activity leading to the alleged incident?

3.2.3.3. What allegedly occurred, to include the use of known cyberspace capabilities to create or facilitate the alleged incident?

3.2.3.4. When did the alleged incident occur?

3.2.3.5. Where did the alleged incident occur, to include what infrastructure may have been employed or impacted?

3.2.4. Follow-up Reporting. As significant additional information is obtained, commanders and task force leaders provide updates to the initial reports through command and servicing judge advocate or legal advisor channels to the CDRUSCYBERCOM.

3.2.5. Higher Headquarters Action. Higher authorities receiving an initial report of a reportable incident shall:

3.2.5.1. Report as essential elements of information (EEI) all reportable incidents by opposing forces, as well as policies, attitudes, and practices which may lead to violations of the law of war. EEI shall be listed as part of Appendix 1 to Annex B (Intelligence) to Operation Order (OPORD).

3.2.5.2. Forward the initial and follow-up reports, by the most expeditious means available, through command and servicing judge advocate or legal advisor channels to USCYBERCOM (Attn: J3/J006).

3.2.6. United States Cyber Command (USCYBERCOM) Action.

3.2.6.1. USCYBERCOM J3 submits a message report, as expeditiously as possible, for all reportable incidents to the Joint Staff, the Office of the Secretary of Defense, United States Special Operations Command, if applicable, and relevant Secretaries of the Military Departments. Normally, an OPREP-3 operational report is required IAW Chairman, Joint Chiefs of Staff Manual (CJCSM) 3150.05D, *Joint Reporting System Situation Monitoring Manual*, when an incident of significance has occurred or where national interest is indicated or has not been determined.

3.2.6.2. USCYBERCOM J3 provides the Joint Staff J1 with copies of all incident reports of reportable incidents committed by or against members of (or persons accompanying or serving with) U.S. Armed Forces, or against their property that it receives from subordinate commands.

3.3. Investigating Law of War Allegations.

3.3.1. Unit or Task Force Headquarters Action. Subject to operational constraints, commanders or task force leaders take appropriate measures to preserve on-scene evidence and report all reportable incidents to their appropriate service investigatory agency for investigation (i.e., U.S. Army Criminal Investigation Command (USACIDC); Air Force Office of Special Investigations Command (AFOSI); and Naval Criminal Investigations Service (NCIS)).

3.3.1.1. If the appropriate service investigatory agency cannot or will not investigate, commanders shall appoint an investigation to be conducted pursuant to service regulations and USCCI 1030-01, *Military Justice and Adverse Administrative Actions*. The commander appoints an investigation pursuant to the service regulation covering the majority of the personnel allegedly involved in the reportable incident.

3.3.1.2. Upon completion of an investigation conducted by CNMF, JFHQ-DODIN, the JFHQ-C, or the SCC, servicing judge advocates or legal advisors, ICW USCYBERCOM SJA, will conduct a legal review of the investigation before the submission of the report of investigation and final resolution to CDRUSCYBERCOM.

3.3.1.3. CNMF, JFHQ-DODIN, the JFHQ-Cs, and the SCCs track investigations and updates, and provide reports of investigation and final resolutions to CDRUSCYBERCOM, Attn: J006.

3.3.2. United States Cyber Command (USCYBERCOM) Action.

3.3.2.1. USCYBERCOM SJA conducts a final review of any reports of investigation and final resolutions, and submits to CDRUSCYBERCOM for final approval.

3.3.2.2. USCYBERCOM CoS provides the Joint Staff J1 with copies of all final reports of investigation of reportable incidents committed by or against members of (or persons accompanying or serving with) U.S. Armed Forces, or against their property that it receives from subordinate commands.

3.4. Legal Guidance and Review.

3.4.1. Legal advisors assigned to USCYBERCOM, CNMF, JFHQ-DODIN, the JFHQ-Cs, the SCCs, and JTFs provide advice and counsel during all stages of operations planning and execution concerning law of war compliance. Command legal advisors should attend planning and operations-related conferences or events for military operations and exercises, as appropriate.

3.4.2. Legal advisors assigned to USCYBERCOM, CNMF, JFHQ-DODIN, the JFHQ-Cs, the SCCs, and JTFs provide advice and counsel for any investigation into reportable incidents and during the preparation of reports pertaining to such investigations.

3.4.3. USCYBERCOM SJA forwards reports of reportable incidents involving allegations of war crimes committed by U.S. civilians, contractors, or subcontractors assigned to or accompanying military forces of their respective Military Department, or their dependents, to the General Counsel DOD, for review for potential prosecutorial action under the criminal jurisdiction of the United States, pursuant to Sections 2441, 2442, or 3261 of Title 18, U.S.C., or other provisions of U.S. law.

3.5. **Periodic Policy Review.** No less than every two years, J3 and J5, ICW the SJA, review all operational plans, policies, and rules of engagement to ensure compliance with domestic and international law, DOD policy, and this instruction.

3.6. **Other Applicable Reporting and Investigation Requirements.** In addition to the reporting and investigation requirements required by DODD 2311.01 and this instruction, comply with other applicable requirements and procedures as required.

3.6.1. Incidents constituting "friendly fire" require compliance with DODI 6055.07, *Mishap Notification, Investigation, Reporting, and Record Keeping*.

3.6.2. Incidents of suspected or alleged violation of DOD policy, procedures, or applicable law relating to intelligence interrogations, detainee debriefings, or tactical questioning for which there is credible information require compliance with DODD 3115.09, *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*.

3.6.3. Incidents of questionable intelligence activities or S/HSMs require compliance with DODD 5148.13.

ATTACHMENT 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

10 United States Code (U.S.C.) § 164
10 U.S.C. § 362
10 U.S.C. § 396
10 U.S.C. § 801-946 (Uniformed Code of Military Justice (UCMJ))
18 U.S.C. §§ 2441, 2442
18 U.S.C. § 3261 (Military Extraterritorial Jurisdiction Act (MEJA))
Geneva Convention Relative to the Protection of Civilian Persons in Time of War of August 12, 1949
Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949
Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of August 12, 1949
Geneva Convention for the Amelioration of the Condition of Wounded and Sick in Armed Forces in the Field of August 12, 1949
DODD 2310.01E, *DoD Detainee Program*, incorporating Change 2, 18 September 2020
DODD 2311.01, *DOD Law of War Program*, 2 July 2020
DODD 3000.03E, *DOD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy*, incorporating Change 2, 31 August 2018
DODD 3000.09, *Autonomy in Weapons Systems*, November 12, 2012, incorporating Change 1, 8 May 2017
DODD 3115.09, *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, incorporating Change 3, 29 October 2020
DODD 5000.01, *The Defense Acquisition System*, 9 September 2020
DODD 5122.05, *Assistant to the Secretary of Defense for Public Affairs (ATSD(PA))*, 7 August 2017
DODD 5148.13, *Intelligence Oversight*, 26 April 2017
DODI 1000.01, *Identification (ID) Cards Required by the Geneva Conventions*, incorporating Change 2, 4 June 2018
DODI 3020.41, *Operational Contract Support (OCS)*, incorporating Change 2, 31 August 2018
DODI 5505.03, *Initiation of Investigations by Defense Criminal Investigative Organizations*, incorporating Change 2, 13 February 2017
DODI 5525.11, *Criminal Jurisdiction Over Civilians Employed By or Accompanying the Armed Forces Outside the United States, Certain Service Members, and Former Service Members*, 3 March 2005
DODI 6055.07, *Mishap Notification, Investigation, Reporting, and Record Keeping*, incorporating Change 1, 31 August 2018
DODM 8910.01, Volume 1, *DOD Information Collections Manual: Procedures for DOD Internal Information Collections*, incorporating Change 2, 19 April 2017
Office of the General Counsel of the Department of Defense, *DOD Law of War Manual*, June 2015, as amended
Chairman, Joint Chiefs of Staff Instruction (CJCSI) 5810.01D, *Implementation of the DOD Law of War Program*, 30 April 2010
CJCSM 3150.05D, *Joint Reporting System Situation Monitoring Manual*, 31 January 2011
CJCSM 6510.01B, *Cyber Incident Handling Program*, 10 July 2012

USCCI 1030-01, *Military Justice and Adverse Administrative Actions*, 30 July 2020
 Army Field Manual 6-27/Marine Corps Tactical Publication 11-10C, *The Commander's Handbook on the Law of Land Warfare*, August 2019
 Marine Corps Order 3300.4A, *Marine Corps Law of War Program*, 9 January 2014
 Air Force Instructions 51-401, *The Law of War*, 3 August 2018
 Air Force Policy Directive 51-4, *Operations and International Law*, 24 July 2018
 Secretary of the Navy Instruction 3300.1C, *Department of the Navy Law of War Program*, 28 May 2009

Acronyms

CDRUSCYBERCOM	Commander, United States Cyber Command
CDRUSSOCOM	Commander, United States Special Operations Command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CNMF	Cyber National Mission Force
CO	Cyberspace Operations
CoS	Chief of Staff
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
EEI	elements of information
IAW	in accordance with
ICW	in coordination with
IG	Inspector General
IOPM	Intelligence Oversight Program Manager
J006	USCYBERCOM Office of the Staff Judge Advocate
J2	Director of Intelligence
J3	Director of Operations
J5	Director of Plans and Policy
J7	Director of Exercises and Training
JFHQ-C	Joint Force Headquarters – Cyberspace
JFHQ-DODIN	Joint Force Headquarters – Department of Defense Information Network
JTF	Joint Task Force
KSA	knowledge, skills, and abilities
MEJA	Military Extraterritorial Jurisdiction Act
NLT	no later than
NLW	Non-Lethal Weapons
OCS	Operational Contract Support
OPR	Office of Primary Responsibility
S/HSM	Significant or Highly Sensitive Matter
SCC	Service Component Command
SecDef	Secretary of Defense
SJA	Staff Judge Advocate
U.S.	United States
U.S.C.	United States Code

USCYBERCOM
USCCI

United States Cyber Command
United States Cyber Command Instruction

Terms

Credible Information. Information that a reasonable military commander would believe to be sufficiently accurate to warrant further review of the alleged violation. The totality of the circumstances is to be considered, including the reliability of the source (e.g., the source's record in providing accurate information in the past and how the source obtained the information), and whether there is contradictory or corroborating information.

Law of War. The treaties and customary international law binding on the United States that regulate: the resort to armed force; the conduct of hostilities and the protection of war crimes in international and non-international armed conflict; belligerent occupation; and the relationships between belligerent, neutral, and non-belligerent States. Sometimes also called the "law of armed conflict" or "international humanitarian law," the law of war is specifically intended to address the circumstances of armed conflict. Consult the DOD Law of War Manual for an authoritative statement on the law of war.

Reportable Incident. An incident that a unit commander or other responsible official determines, based on credible information, potentially involves: a war crime; other violations of the law of war; or conduct during military operations that would be a war crime if the military operations occurred in the context of an armed conflict. The unit commander or responsible official need not determine that a potential violation occurred, only that credible information merits further review of the incident.

Significant or Highly Sensitive Matter (S/HSM). An intelligence or intelligence-related activity (regardless of whether the intelligence or intelligence-related activity is unlawful or contrary to an Executive Order (E.O.), Presidential directive, Intelligence Community Directive (ICD), or DOD policy), or serious criminal activity by intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of intelligence activities. Such matters might involve actual or potential: (a) Congressional inquiries or investigations; (b) adverse media coverage; (c) impact on foreign relations or foreign partners; or (d) systemic compromise, loss, or unauthorized disclosure of protected information.

War Crime. Serious violations of the law of war that generally have been committed intentionally, such as murder, torture, rape, pillage, extensive and wanton destruction of property without justification, and intentionally directing attacks against the civilian population or civilians protected as such. "War crimes" may be defined differently in other contexts for other legal purposes.