BY ORDER OF THE COMMANDER
512TH AIRLIFT WING

512 AIRLIFT WING INSTRUCTION
10-701

7 MAY 2019
Certified Current, 16 MAY 2024
Operations

OPERATIONS SECURITY (OPSEC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-publishing.af.mil/**.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 512 OSF/OSTX

Certified by: 512 AW/CC
(Col Craig C. Peters)

Supersedes: 512 AW OPSEC Policy Memo 2016

Pages: 6

This instruction implements Air Force Policy Directive (AFPD) 10-7, *Information Operations*, 4 August 2014 and Air Force Instruction (AFI) 10-701, *Operations Security (OPSEC)*, 8 June 2011. It applies to all 512 AW personnel, and establishes responsibilities and guidelines for conducting the 512 AW OPSEC program. This instruction augments, but does not supersede, any AFI or Air Force Reserve Command (ARC) Supplement. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, 1 March 2008 and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/gcss-af61a/afrims/afrims/rims.cfm**. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847 to 512 OSS/OSTX, Building 270, Room 123, Dover AFB, DE 19902.

SUMMARY OF CHANGES

This instruction replaces the Wing OPSEC Policy Memorandum and replaces it with a publication in accordance with AFI 33-360, *Publications and Forms Management*, 1 December 2015.

1. General Guidelines:

1.1. The purpose of OPSEC is to identify, evaluate and protect critical or sensitive information, relating to the 512 AW daily and wartime activities. OPSEC utilizes a

continuous five-step process to reduce vulnerabilities by eliminating or reducing successful adversary collection and exploitation of critical information. Military adversaries, criminals, terrorists and others continually seek to exploit our information vulnerabilities. Application of OPSEC countermeasures is essential to the protection of our critical information, and failure to protect this information could put the mission and our families at risk.

1.2. OPSEC procedures should be closely coordinated with base security and information protection disciplines to ensure uniformity. Commanders at every level must take an active role in the OPSEC program to ensure its success.

1.3. Failure to comply with parent and local OPSEC guidance could result in punishment under Article 92 of the UCMJ or civil equivalent.

2. Roles and Responsibilities:

2.1. **512 AW OPSEC Program Managers will:**

2.1.1. Work in coordination with 436 AW OPSEC Program Managers (PM).

2.1.2. Evaluate (at a minimum, annually) the effectiveness of the Wing Commander's guidance for 100% shredding of all internally generated paperwork.

2.1.3. Assist wing organizations to ensure compliance with this guidance.

2.1.4. Provide unit OPSEC coordinators with recurring OPSEC awareness training, guidance and materials for unit personnel.

2.1.5. Maintain Wing Critical Information and Indicator List (CIIL) as well as training and awareness products on 512 AW OPSEC SharePoint site.

2.1.6. Accomplish the wing OPSEC Management Internal Control Toolset (MICT) checklist annually as directed by the Wing Inspector General Inspections (IGI).

2.1.7. Be considered as either permanent members or advisors to the 512 AW Wing Inspection Team.

2.1.8. Work with 512 Public Affairs to review information intended for public release.

2.2. **Unit Commanders will:**

2.2.1. Appoint primary and secondary unit OPSEC coordinators to support unit OPSEC awareness and training, and to support the OPSEC PMs. Select OPSEC coordinators that are familiar with all aspects of the unit's mission to ensure effective oversight of the unit's OPSEC program and can effectively provide inputs to the wing OPSEC PMs.

2.2.2. Ensure all unit members are aware of their unit OPSEC coordinators and/or the wing OPSEC PMs by posting this information in a highly visible location within the unit.

2.3. **Unit OPSEC Coordinators/POCs will:**

2.3.1. Complete required OPSEC training and forward completion documentation to the wing OPSEC PMs.

2.3.2. Continuously review their programs to mitigate the release of unclassified information affecting the unit's mission, personnel or equipment.

2.3.3. Ensure current unit OPSEC CIIL is posted next to all communication devices.

2.3.4. Continuously evaluate the work environment ensuring OPSEC is incorporated into daily operations and ensure procedures are in place to control the distribution of wing and unit critical information.

2.3.5. Advise their unit commander and his/her staff on OPSEC issues. Forward any OPSEC issues to the wing PMs.

2.3.6. As required, assist the wing PMs in conducting recurring OPSEC awareness and assessment activities.

2.3.7. Monitor both external-facing and internal unit web pages, publications and other venues that disseminate information to unit personnel ensuring protection of critical information.

2.3.8. Ensure their organization conducts an annual content vulnerability analysis if they maintain any external web or SharePoint sites that do not require a DoD Common Access Card.

2.3.9. Notify the wing PM if updating their unit-specific CIIL or if any unauthorized release of critical information is brought to their attention.

2.3.10. Provide OPSEC guidance and materials to members' families to ensure they understand their role in protecting the wing's critical information. Deployed personnel and their families are especially susceptible to inadvertently divulging our critical information via their electronic communications.

2.3.11. Notify AFOSI immediately when becoming aware of an unsolicited request (verbal, electronic or written) for critical or sensitive information.

2.3.12. Ensure all information that is to be released to the public is coordinated with the 512 AW Public Affairs Office.

2.4. **512 AW Public Affairs Office.** Public Affairs has a unique position in protecting critical information while at the same time complying with the Department of Defense (DoD) Principles of Information. To facilitate the protection of critical information during day-to-day operations, the Public Affairs office will:

2.4.1. Appoint a primary and alternate OPSEC coordinator. Appointed Public Affairs OPSEC coordinators will also serve as OPSEC coordinators for the Wing Staff Agencies.

2.4.2. Inform the wing OPSEC PM of higher headquarters policy and guidelines on critical information approved for release to the public.

2.4.3. Ensure media releases do not contain critical information outside of the scope of information approved for release by higher headquarters. The protection of critical information is always important and risk management must be utilized to mitigate the adverse effects to the mission or exercises.

2.4.4. Consult the wing OPSEC PMs for assistance and utilize the current 512 AW CIIL during the coordination process for all information released to the public to ensure critical information and indicators are not made available for public consumption.

2.5. **All 512 AW Personnel will:**

2.5.1. Know and protect wing and unit critical information. This information can be found on the OPSEC CIIL posted by all computers and phones.

2.5.2. Immediately report to wing OPSEC PMs or unit OPSEC coordinators if an unsolicited request (verbal, electronic or written) is received for critical or sensitive information.

2.5.3. Verify the credentials of any unfamiliar person entering non-public facilities (mission essential, restricted, controlled entry areas, etc.).

2.5.4. Protect personal information IAW the Privacy Act of 1974, DoD 5400.11-R, DoD Privacy Act Program and AFI 33-332 (specifically para 1.1.11.4), Air Force Privacy and Civil Liberties Program.

2.5.5. Scrutinize all information posted on social or internet-based bulletin boards for critical or sensitive information.

2.5.6. Notify their supervisor and/or OPSEC coordinator if any critical information is discovered on public internet sites.

2.5.7. Not publish or distribute any documents (paper or electronic) that contain critical information without first soliciting the advice of their unit OPSEC coordinator, wing OPSEC PMs and/or the Public Affairs office.

3. 512 AW Daily OPSEC Countermeasures:

3.1. Make OPSEC practices a way of life.

3.1.1. Practice good OPSEC both on and off duty, when engaged in direct communication, and also when using social media and internet-based networking.

3.1.2. Encourage others and family members to protect critical information and indicators.

3.1.3. Do not post entries on social networking sites that describe current or impending deployments, aircraft and troop movements, or other pieces of critical information.

3.1.4. Never tag photos with geographical location or use location-based social networking applications when deployed, during training, or while on duty where presenting this information could damage operations.

3.1.5. Turn off the GPS function of personally owned smartphones and smart devices while engaged in operational missions or major exercises.

3.2. Prevent inadvertent disclosure of our critical information.

3.2.1. 100% Shred Policy. All internally generated office paperwork, which is not publicly available, regardless of classification, must be shredded prior to being recycled.

3.3. Safeguard our communication.

3.3.1. Ensure personnel receiving access to critical or sensitive information have a “need to know” prior to releasing or transmitting this information.

3.3.2. Use the most secure means of communication available when releasing or transmitting critical information.

3.3.3. Encrypt. If Privacy Act, PII, FOUO, Controlled Unclassified Information or Critical Information must be transmitted via email, DoD Public Key Infrastructure encryption will be used.

CRAIG C. PETERS, Col, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

JP 3-13.3, *Operations Security*, 29 June 2006

AFPD 10-7, *Information Operations,* 4 August 2014

AFMAN 33-363, *Management of Records*, 1 March 2008

AFI 10-701, *Operations Security (OPSEC),* 8 June 2011

AFRC Supplement to AFI 10-701, *Operations Security (OPSEC),*13 January 2012

Terms

Adversary—An individual, group, organization or government that must be denied critical information and indicators. Synonymous with competitor/enemy.

Critical Information—Specific facts about friendly intentions, capabilities, or activities needed by adversaries to plan and act effectively against friendly mission accomplishment.

CIIL—A combination of mission-specific facts, evidence, and detectable actions from which an adversary or potential adversary could accurately deduce friendly activity, capability, or intent to a level of unacceptable risk to mission accomplishment. The key output of the "Identify Critical Information" step in the OPSEC process.

OPSEC—An information related capability that preserves friendly essential secrecy by identifying, controlling, and protecting critical information and indicators that would allow adversaries or potential adversaries to identify and exploit friendly vulnerabilities leading to increased risk and potential mission failure.

OPSEC Countermeasure—Planned action to affect collection, analysis, delivery, or interpretation of information. OPSEC countermeasures include all activities that affect content and flow of critical information and indicators from collection to the decision maker. Countermeasures are generally offensive in nature and may require additional approval authorities and review criteria associated with choice of means employed.

OPSEC Indicator—Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

Vulnerability—An exploitable condition in which the adversary has sufficient knowledge, time, and available resources to thwart friendly mission accomplishment or substantially increase operational risk.