BY ORDER OF THE COMMANDER
ELLSWORTH AIR FORCE BASE

AIR FORCE INSTRUCTION 10-701

19 JULY 2023

Operations

OPERATIONS SECURITY (OPSEC)/ SIGNATURE MANAGEMENT (SM)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 28BW/CCT

Certified by: 28BW/CC
(Col Derek C. Oakley)

Pages: 7

This publication implements Air Force Instruction (AFI) 10-701, *Operations Security (OPSEC)*. It applies to all 28th Bomb Wing (BW) personnel and establishes responsibilities and guidelines for conducting the 28 BW Operations Security (OPSEC) program. This instruction augments, but does not supersede, any or Air Force Global Strike Command (AFGSC) Supplement. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFI 33-322, *Records Management and Information Governance Program*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://afrims.cce.af.mil**. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the Air Force (AF) Form 847, *Recommendation for Change of Publication*; route AF Form 847 to 28 BW/CCT, Building 7925, Room 235, Ellsworth AFB, SD 57706.

1. Overview.

1.1. The purpose of OPSEC is to identify, evaluate and protect critical or sensitive information, relating to the 28 BW 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 must 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. Failure to comply with parent and local OPSEC guidance could result in punishment under Article 92 of the Uniform Code of Military Justice (UCMJ) or civil equivalent.

2. Roles and Responsibilities.

2.1. 28 BW OPSEC Signature Managers (SM) Will:

2.1.1. Work in coordination with AFGSC 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 28 BW groups, squadrons, and base tenant 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 28 BW 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 permanent members of the 28 BW Wing Inspection Team.

2.1.8. Work with 28 BW/Public Affairs (PA) 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 wing OPSEC SMs. Select OPSEC coordinators that are familiar with all aspects of the unit's mission to ensure effective oversight of the unit's OPSEC program. Coordinators must have two years on station retainability and E-4 or O-2 at a minimum.

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

2.3. Unit OPSEC Coordinators Will:

2.3.1. Complete required OPSEC coordinator training (OPSE-1301) within 90 days of appointment and forward completion documentation to the wing OPSEC SMs.

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 Cue Card is posted next to phones and computers.

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 SMs.

2.3.6. As required, assist the wing SMs 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 the unit personnel to ensure protection of critical information and indicators as outlined in the monthly OPSEC unit self-assessment checklist.

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 Department of Defense (DoD) Common Access Card (CAC).

2.3.9. Coordinate with wing SMs when updating their unit specific CIILs prior to commander signature. Provided record copy upon commander signature.

2.3.10. When an unsolicited or unauthorized release of critical/sensitive information (verbal, electronic or written) occurs, immediately (or no later than) 1 business day, notify Air Force Office of Special Investigation (AFOSI) and wing SMs.

2.3.11. Provide OPSEC guidance and materials to members' families to ensure they understand their role in protecting the wing's critical information.

2.3.12. Ensure all information that is to be released to the public is coordinated with the 28 BW PA Office.

2.4. 28 BW PA Office. PA has a unique position in protecting critical information while at the same time complying with the DoD Principles of Information. To facilitate the protection of critical information during day-to- day operations, the PA office will:

2.4.1. Appoint a primary and alternate OPSEC coordinator within PA to assist wing SMs monitoring online/social media content.

2.4.2. Inform the wing OPSEC SMs of higher headquarters policy and guidelines that change 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.

2.4.4. Consult the wing OPSEC SMs for assistance and utilize the current 28 BW CIIL during the coordination process for all information released to the public to ensure critical information and the indicators themselves are not made available for public consumption.

2.4.5. Coordinate Higher Head Quarters (HHQ)-directed releases with affected units to identify perceived risks from the BW and/or Sq levels and correspond with HHQ regarding any objections to publication of specific info from a CIIL.

2.5. All 28 BW Personnel Will:

2.5.1. Know and protect wing and unit critical information. Utilize and post the 28 BW Critical Information Cue Card near all Non-Secure Internet Protocol Router (NIPR) computers and unclassified phones.

2.5.2. Immediately report to wing OPSEC SMs 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 In Accordance With (IAW) the Privacy Act of 1974, DoD 5400.11-R, *Department of Defense Privacy Program* and AFI 33-332, *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 SMs and/or the PA office.

3. 28 BW 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 when using social media and internet-based networking.

3.1.2. Encourage 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. When engaged in operational missions or major exercises turn off the personal and unnecessary government phones and smart devices, at a minimum confirm Global Positioning System (GPS), Wireless Fidelity (WIFI), Bluetooth functions are deactivated and no “Air tag” type devices are present.

3.2. Prevent inadvertent disclosure of our critical information.

3.2.1. 100% Shred Policy. All internally generated office paperwork, office notes, 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. Encryption. DoD Public Key Infrastructure (PKI) encryption will be used for emails with Controlled Unclassified information (CUI) or Personal Identifiable Information (PII)/Protected Health Information (PHI) when sent to addresses that are not @us.af.mil, @usspacecom.mil, or @spaceforce.mil domains.

DEREK C. OAKLEY, Colonel, USAF
Commander, 28th Bomb Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 10-701, *Operations Security (OPSEC)*, 24 July 2019

AFI 33-322, *Records Management and Information Governance Program*, 27 Jul 2021

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 9 March 2020

DAFI 90-160, *Publications and Forms Management*, 13 April 2022

DoD 5400.11-R, *Department of Defense Privacy Program*, 29 October 2014

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AF—Air Force

AFGSC—Air Force Global Strike Command

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

BW—Bomb Wing

CAC—Common Access Card

CIIL—Critical Information and Indicator List

CUI—Controlled Unclassified Information

DAFI—Department of the Air Force Instruction

DoD—Department of Defense

GPS—Global Positioning System

HHQ—Higher Headquarters

IAW—In Accordance With

IGI—Inspector General Inspections

NIPR—Non-Secure Internet Protocol Router

MICT—Management Internal Control Toolset

OPR—Office of Primary Responsibility

OPSEC—Operations Security

PA—Public Affairs

PHI—Protected Health Information

PII—Personal Identifiable Information

PKI—Public Key Infrastructure

PM—Program Managers

RDS—Records Disposition Schedule

SM—Signature Managers

UCMJ—Uniform Code of Military Justice

WIFI—Wireless Fidelity

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—**Critical Information and Indicators List.** 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.