BY ORDER OF THE
19TH AIRLIFT WING COMMANDER

LITTLE ROCK AFB INSTRUCTION

10-701

20 JANUARY 2023

OPERATIONS

OPERATION SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading.

RELEASABILITY: There are no restrictions to releasing this publication.

OPR: 19 AW/XP

Certified by: 19 AW/CC
(Mr. Ronald Decker)
Pages: 166

This instruction applies to all 19th Airlift Wing units, mission partners, tenant units and contractors assigned to, or visiting Little Rock AFB (LRAFB). It describes the OPSEC process and discusses integration of OPSEC into Air Force (AF) plans, operations and support activities. 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 Forms 847 from the field through the appropriate chain of command. Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the AF.

1. Overview.

1.1. The purpose of OPSEC is to identify, evaluate and protect critical or sensitive information, relating to the 19 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. 19 AW Commander will:

2.1.1. Ensure coordination with the organization's command-level, other organizations and tenant(s) on the installation to ensure the protection of mission critical activities and capabilities.

2.1.2. Appoint in writing a primary OPSEC Signature Manager (OSM) at grades no lower than O-3, E-7 or GS-12 and an alternate OSM at grades no lower than O-1, E-6 or GS-9 from the 19 AW/XP office.

2.1.2.1. Ensure OSM is appointed for no less than two-years for the AF to optimize their training investment.

2.1.3. Ensure measures are in place to manage the 19 AW and assigned tenant wings' Operational Signatures and prevent disclosure of critical information and indicators as described in each wings' Critical Information and Indicator List (CIIL).

2.1.4. Ensure group and squadron commanders appoint OPSEC Coordinators to implement and enhance the effectiveness of OPSEC within the wing and support the Wing OSM. Appointment for tenant wings/units is at the discretion of each of those Wing Commanders.

2.1.5. Ensure OPSEC education and training is available for all assigned military personnel, civilians, and Department of Defense (DoD) contractors. Training will consist of an introduction to the OPSEC Process, the definition of OPSEC and its purpose, identifying critical information, understanding one's role in protecting critical information, and a basic overview of adversarial threats to the Air Force's critical information.

2.1.6. Ensure the annual OPSEC Report is completed, signed, and forwarded to each unit's MAJCOM OPSEC Program Manager (PM) on or before the established MAJCOM due date.

2.1.7. Ensure contract requirement owners coordinate with the OSM, the contracting office and other stakeholders to ensure mission critical information and indicators are not included in publicly available contract documents.

2.1.8. Ensure implementation of wing-level OPSEC guidance to incorporate and institutionalize OPSEC concepts into relevant documents and day-to-day and contingency operations.

2.2. Group and Squadron Commanders:

2.2.1. Appoint OPSEC Coordinator(s) to implement and enhance the effectiveness of OPSEC within the organization and support to the organization's OSM. Select OPSEC

Coordinators with a current and favorable Secret clearance and familiar with all aspects of the unit's mission to ensure effective oversight of the unit OPSEC program.

2.2.1.1. Ensure each unit's appointment letter is updated and provided to the 19 AW OSM (19 AW/XP) within 15 workdays of appointment and member has received training within 90 days of appointment as outlined in AFI 10-701, Chapter 4.

2.2.2. Ensure unit OPSEC Coordinators are taking a proactive and effective approach to increase awareness with unit members (i.e., Squadron In-processing, Commanders Calls, etc.)

2.2.2.1. Ensure all unit members are aware of their unit OPSEC Coordinators and the Wing OSM.

2.2.2.2. Ensure unit OPSEC Coordinator and Wing OSM contact information is in a highly visible location within the unit and associated facilities.

2.2.2.3. Reinforce the importance of OPSEC, the 19 AW CIIL and units' CIIL into daily operations.

2.2.3. Group OPSEC Coordinators will work with unit OPSEC Coordinators and ensure subordinate squadron's OPSEC processes correlate with the group's mission.

2.2.4. Ensure unit OPSEC Coordinators conduct OPSEC reviews of organizational documents and photographs in coordination with 19 AW/PA prior to public release, as required.

2.3. 19 AW OPSEC Signature Manager (OSM) serves as the 19 AW/CC's representative regarding OPSEC and is the POC for Signature Management related issues between the HQ AMC OPSEC PM and the 19 AW subordinate organizations and tenant wing OSMs (as required). The 19 AW OSM will:

2.3.1. If not already trained, attend the AF OPSEC Course within 90 days of appointment. See AFI 10-701, para 2.22 for detailed list of OSM duties and responsibilities.

2.3.2. Work with units, OSI, Threat Working Group (TWG), Intelligence personnel and tenant wing OSMs to review/update all applicable CIIL and countermeasures annually.

2.3.3. Review and assess the effectiveness and efficiency of OPSEC within the 19 AW annually. Include currency and effectiveness of subordinate organization's procedures to control critical information and associated indicators. See AFI 10-701, para 5.2.

2.3.3.1. Conduct annual staff assistance visits (SAV) with unit OPSEC Coordinators to ensure compliance with directives. Reference this document, Attachment 3 for OPSEC Coordinator Checklist. Provide written results of the SAV to unit Commanders within 5 workdays of the visit.

2.3.4. Coordinate with contract requirement owners and review contract documents as they are submitted to the OSM from 19th Contracting Squadron (19 CONS) to ensure publicly available contract documents do not include unit critical information and indicators.

2.3.5. Integrate OPSEC into all plans (operational, functional, deployment and exercise).

2.3.6. Assist Wing Inspection Team (WIT) members and exercise planners in developing Master Scenario Events List (MSEL) and measures of performance to train organization personnel in the application or execution of countermeasures.

2.3.6.1. Evaluate OPSEC practices during wing level exercises through spot inspections in units as part of the WIT as well as evaluating the established measures of performance.

2.3.7. Using the OPSEC process, identify signatures, critical information and indicators and assess the risk for each of the organization's activities relating to the planning, development, deployment and movement of equipment, personnel, weapon systems and capabilities whether the activity is planned, conducted or supported, documenting all mitigation efforts.

2.3.7.1. Reference this document, **Attachment 2**, OPSEC Process Milestones, to assist in the OPSEC process. Document mitigation efforts during the SAV in the OPSEC Inspection Checklist, "Unit OPSEC Awareness" section.

2.3.8. Identify current threats that have a capability and intent to obtain and exploit the critical information and indicators within the organization's CIIL by requesting local threat update from OSI as required.

2.3.9. Ensure the implementation of OPSEC measures and countermeasures into organizational activities to reduce vulnerabilities and indicators, verified during a unit's annual SAV inspection or unit vertical inspection (UVI), if conducted.

2.3.10. Coordinate the integration of OPSEC measures and countermeasures with other information-related capabilities and the organization's command-level, other organizations and tenant(s) on the installation to ensure the protection of mission critical activities and capabilities.

2.3.11. Chair the OPSEC Working Group (OWG); see **Table 4.1** for OWG members.

2.3.12. Provide an in-person training brief to OWG members and OPSEC Coordinators identified on their appointment letters. This will be focused on their role in the 19 AW in addition to the required training outlined in AFI 10-701, Table 4.1.

2.3.12.1. Track training of OPSEC Coordinators and OWG members.

2.4. 19 AW OPSEC Coordinators (Group/Squadron) and tenant appointed Coordinators will:

2.4.1. Actively facilitate the implementation of OPSEC throughout their respective group and/or squadron.

2.4.1.1. Be familiar and comply with **Attachment 3**, this document, Unit OPSEC Coordinator Checklist as that will be used during the annual SAV to ensure compliance with directives.

2.4.2. Assist in developing guidance and implementing countermeasures to mitigate the risk of potential adversary exploitation of critical information and indicators.

2.4.3. Distribute the 19 AW/CC's and/or tenant wing CC's OPSEC guidance (e.g., CIIL, memorandums) as required.

2.4.4. Publish and disseminate a unit CIIL within the unit and submit a copy to the 19 AW OSM as required.

2.4.5. Immediately notify the wing OSM if updating their unit CIIL or if any unauthorized release of critical information is brought to their attention.

2.4.6. Complete the required OPSEC training (ref: Chapter 4, Table 4.1 of AFI 10- 701) within 90 days of appointment and provide certificates to the OSM immediately after completion.

2.4.7. Serve as the unit's POC for questions related to the OPSEC category of the CUI program. Elevate to the 19 AW OSM if assistance is required.

2.4.8. Annually provide unit's training material to the OSM for review.

2.4.9. Maintain a record of personnel trained and submit to the OSM annually.

2.4.10. Establish and maintain an organization OPSEC continuity binder (either electronic or hard copy) that consists of unit appointment letter, wing or unit CIIL, unit OPSEC Coordinator training certificates, unit initial/annual tracker, and (optional) unit policy guidance letter.

2.4.11. Ensure annual OPSEC reviews of organization owned, operated, or controlled external facing media sites are conducted to confirm critical information and indicators are not being made available to the public.

2.4.12. Assist WIT members and exercise planners in developing the MSEL and measures of performance to train unit personnel in the application or execution of countermeasures as requested by OSM.

2.4.13. Provide mission-oriented OPSEC education that may be directed by the commander/ director to address specific events not covered by annual OPSEC education such as CUI breaches, change of mission, updates to the CIIL, recurring OPSEC disclosures, new threats and/or vulnerabilities, and countermeasures. Mission-oriented OPSEC education includes, at a minimum, updated threat information, changes to CIIL, new procedures, and/or OPSEC measures implemented, altered or deleted by the organization.

2.5. 19 AW Intelligence. IAW *19 OSS/IN Support to 19 AW OPSEC Program* MFR, 19 AW INTEL will provide OPSEC awareness of critical information and indicators pertaining to their deployed locations prior to member deploying. Theater-specific critical information and indicators that require protection can be obtained from the deployed location's OPSEC Program Manager or OPSEC Signature Manager.

2.6. 19 AW Public Affairs Office. 19 AW/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 19 AW/PA office will:

2.6.1. If not previously completed, member must complete Air Force Identity Management course. The course is required to be completed within 90 days of appointment of public affairs duties. The Identity Management Course is located on the Joint Knowledge Online website **https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf**.

Provide 19 AW OSM (19 AW/XP) a copy of the certificate of completion once course is completed.

2.6.2. Ensure OPSEC considerations are included in Public Affairs Security Policy Review and all other public information release processes and send the review checklist to the OSM annually for review.

2.6.3. Ensure annual OPSEC reviews of 19 AW owned, operated, or controlled external facing media sites are conducted to confirm critical information and indicators are not being made available to the public.

2.6.4. 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.

2.7. All 19 AW Personnel will:

2.7.1. Know and protect the wing's, tenant's, and units' critical information. This information can be found on the 19 AW OPSEC CIIL which is maintained by the group/unit OPSEC Coordinator(s) and on each tenant's OPSEC Site.

2.7.2. Immediately report to the respective wing OSM or unit OPSEC Coordinator(s) if an unsolicited request (verbal, electronic or written) is received for critical or sensitive information.

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

2.7.4. Protect personal information IAW the *Privacy Act of 1974*, DoD 5400.11-R, *DoD Privacy Program* and AFI 33-332 (specifically **para 7.1**), Air Force Privacy and Civil Liberties Program.

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

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

2.7.7. Not publish or distribute any documents (paper or electronic) that contain critical information without first soliciting the advice of their unit OPSEC Coordinator, 19 AW OSM and/or the 19 AW/PA office.

2.7.8. Communicate with family members about the concepts of OPSEC, the inherent risks and dangers associated with social media along with their vital role in OPSEC program. Family members' understanding of OPSEC and participation is critical to mission success and to the personal safety of service members and family members alike.

3. 19 AW Daily OPSEC Countermeasures:

3.1. Incorporate OPSEC practices and techniques into all on and off-duty conduct.

3.1.1. Practice responsible OPSEC both on and off-duty, when engaged in direct communication, and when using social media and internet-based networking. Complacency risks compromising the security of our mission as enough unclassified and

mission-specific information can provide an adversary with a clear picture of the command's vulnerable areas.

3.1.1.1. Direct communication includes, but is not limited to letters, resumes, articles, books, collegiate papers, electronic mail (e-mail), social media postings, web log (blog) postings, internet message board discussions, or other forms of dissemination or documentation. Everyone must do their part to question and secure correspondence to the appropriate level and seek guidance when unsure.

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 appropriately shredded prior to being recycled.

3.3. Safeguard your 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 Controlled Unclassified Information (CUI) or Critical Information must be transmitted via email, DoD Public Key Infrastructure encryption will be used.

4. OPSEC Working Group (OWG):

4.1. The OWG consists of subject matter experts representing a wide range of specialties to provide information, advice, and support to address OPSEC concerns. The OWG is crucial to completing the five-step process for identifying threats and adversaries to help units develop countermeasures to mitigate vulnerabilities.

4.1.1. OWG members will meet as necessary to conduct the OPSEC process for new and existing organization activities or as the 19 AW OPSEC SM deems appropriate.

4.1.1.1. Provide meeting minutes within 10 workdays.

4.1.2. The following positions are designated as OWG Members. All OWG members must possess and maintain a favorable Secret clearance, at a minimum.

Table 1. OPSEC Working Group Members.

Office Symbol	Office Name/Job Title
19 AW/XP	Wing Plans and Programs
19 LRS/LGRDX	Chief, Plans/Integration/Installation Deployment Officer
19 SFS/S5X	Antiterrorism Program Manager
19 SFS	OPSEC Coordinator
19 OG	OPSEC Coordinator
19 MXG	OPSEC Coordinator
19 MSG	OPSEC Coordinator
19 MDG	OPSEC Coordinator
19 CPTS/CC Appointee	Wing Staff Agency Representative
19 AW/PA	Chief/Superintendent/Designee
19 CONS/CC Appointee	OPSEC Coordinator
19 OSS/IN	Intelligence Specialist
19 CS	Cyber Security Specialist
19 CS/SCXK	Base Records/FOIA/Privacy Manager
19 OSS/OSAA	Airfield Manager/Deputy
189 AW OPSEC Program Manager	OPSEC Manager
913 AG OPSEC Program Manager	OPSEC Manager
314 AW OPSEC Program Manager	OPSEC Manager
AFOSI/DET 327/CC Appointee	

Angela F. Ochoa, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

AFI 33-322, *Records Management and Information Governance Program*, March 23, 2020

Prescribed Forms

None

Abbreviations and Acronyms

AF—-Air Force

CIIL—-Critical Information and Indicator List

CUI—-Controlled Unclassified Information

DOD—-Department of Defense

MSEL—-Master Scenario Events List

OPR—-Office of Primary Responsibility

OPSEC—-Operations Security

OSM—-OPSEC Signature Manager

OWG—-OPSEC Working Group

SAV—-Staff Assistance Visits

TWG—-Threat Working Group

UCMJ—-Uniform Code of Military Justice

UVI—-Unit Vertical Inspection

WIT—-Wing Inspection Team

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.

Critical Information and Indicators List (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.

Indicator—Detectable actions and information that can be interpreted and pieced together to reach conclusions or estimates concerning friendly intentions, capabilities, or activities.

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.

Signature Management (SM)—The active defense or exploitation of operational profiles resident at a given military installation. Defense of operational profiles is accomplished by implementing protective SM measures to deny adversary collection of critical information and indicators.

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.

Attachment 2

PROCESS MILESTONES

Figure A2.1. Process Milestones

PROCESS MILESTONES

Step 1: Identify unit processes. Identify and list the unit's most important missions/activities.

Step 2: Flowchart unit processes. Select one of the mission/activity areas and map it with its most important associated event s/processes.

- At this point, this may be a "surface level" flowchart. The OSMs may need to coordinate with SMEs in the following steps to expand the processes appropriately.
- Ensure each event/process is numbered for easier feedback and reference.

A2.3. Step 3: Identify conduits.

- Make a list or legend of known conduits & clarify type (i.e., DSN, VOSIP, personal cell[text/call], app/website, GDSS, NIPR/ SIPR email, personal email, LMR, F2F, etc.).
- Verify with the POCs who are regularly and directly involved with the processes which type(s) of communications that are actually used for each event before proceeding to the next event.

Step 4: Transfer steps & conduits to Process Checklist.

- Ensure each event/process is numbered for identification and reference.
- Ensure any apps or sites that are ***not*** accessed/used on a government-issued device are marked for reference (even if approved).

Step 5: Establish Process Checklist Timing.

- Most importantly, identify D-Day timing. Sometimes it may also benefit comprehension to identify any known "average process times" between stages.

Step 6: Identify process indicators/vulnerabilities.

- Use information gathered from local intel, OSI, SF, intel from SIPR/JWICS reports, etc. to analyze threat to AMC, the specific missions/activities that your unit runs, and identification of potential vulnerabilities to the location of your site (i.e. potential adversaries using open-source data [tail watcher forums, etc.], ability to use telephoto-lens camera to observe base movements, overhead satellites, patterns-of-life deviations, etc.).
- Verify indicators with the POCs who are regularly and directly involved with the processes.

- Assess level of risk for each indicator/vulnerability with help from OPSEC Analysts and/or OPSEC Planners.

Step 7: Identify process input/output systems (with workarounds).

- For example:
  - **CAMS,** aircraft mx for supply, **Why identified?:** May need to work with maintenance work-arounds [such as an **AFTO 349]** if/when associated with sensitive mission/activity.
  - **G081,** aircraft mx, **Why identified?:** May need to work with maintenance to not input information if/when associated with sensitive mission/activity.
  - **GDSS,** functionally owned by 618 AOC, **Why identified?:** May need to process work-arounds with AOC if/when associated with sensitive mission/activity.
  - Fuel Credit Card, fuels, etc.
- Verify potential work-arounds with the POCs who are regularly and directly involved with the processes; some units may need to write these work- arounds, or reference MOAs/MOUs, into an activity's *OPSEC/Signature Management plan.*

Step 8: Identify SME job descriptions.

- Sentence or two to describe the functional area of SMEs, for reference. This may also help re-locate help if functional areas or system names change nomenclatures over time.
- Identify where those SME functional areas may fit in your process(es) and attach to your Checklist(s) for reference.

Step 9: Input process checklists into Signature Management Master Checklist.

- After inputting one mission/activity, the OSM will proceed to map another one and input each into this "list of mapped processes" for reference of the unit's operational profiling.
- This list can be used to more effectively analyze common and most significant risks to the unit's operations, enabling OSMs to provide leadership with options. This constitutes managing signatures.

Attachment 3

UNIT OPSEC COORDINATOR CHECKLIST

Figure A3.1. Unit OPSEC Coordinator Checklist

Unit OPSEC Coordinator Checklist OPR: 19 AW/XP Dec 2021 version				
No.	Question/ Reference	Y/N/NA	Remarks	Est Comp.
1	Has the unit CC appointed an OPSEC Coordinator? Ref. AFI 10 701 para. 2.19.4 LRAFBI 10-701 para. 2.2.1			
2	Do the appointed OPSEC Coordinator(s) possess valid secret clearances? Ref. AFI 10-701 para. 2.17.4 LRAFBI 10-701 para. 2.2.1			
3	Have the OPSEC Coordinator(s) completed required training within 90 days of appointment? Ref. AFI 10-701 para. 2.24.3/Table 4.1/See Note 1 below. LRAFBI 10-701 para. 2.4.6			
4	Are the OPSEC Coordinators ensuring that unit personnel are familiar with the organization critical information, indicators, and threats? Ref. AFI 10-701 para. 2.24.5 LRAFBI 10-701 para. 2.4.3 and para. 2.4.4			
5	Are the OPSEC Coordinators ensuring that unit personnel are protecting all electronic communications containing critical information and indicators? Ref. AFI 10-701 para. 1.8.4/See Note 2 below. LRAFBI 10-701 para. 3.3			
6	Do the OPSEC Coordinators have measures in place to ensure personnel do not publicly disseminate or publish information or imagery displaying critical information? Ref. AFI 10-701 para. 1.8.4/See Note 2 below. LRAFBI 10-701 para. 2.4.10			

7	Do the OPSEC Coordinators assist in developing and recommending guidance and in implementing countermeasures to reduce the risk of exploiting the critical information and indicators? Ref. AFI 10-701 para. 2.24.1 See Note 3 below. LRAFBI 10-701 para. 2.4.2			
8	Do the OPSEC Coordinators help distribute the commander's/director's OPSEC Guidance? Ref. AFI 10-701 para. 2.24.2/See Note 4 below. LRAFBI 10-701 para. 2.4.3.			
9	Are the OPSEC Coordinators providing unit personnel the proper OPSEC education? (OPSEC process, definition of OPSEC, purpose what is critical information, individual's role protecting critical information, general threat to AF's critical information) Ref. AFI 10-701 para. 2.24.5/4.2.1/See Note 6 below. LRAFBI 10-701 para. 2.1.5			
10	Are the OPSEC Coordinators conducting an OPSEC review of organizational documents and photographs as required w/Public Affairs prior to public release as required? Ref. AFI 10-701 para. 2.24.6/See Note 7 below. LRAFBI 10-701 para. 2.2.4			
11	Have the OPSEC Coordinators assisted in the review of unit contracting documents as required to ensure that the unit's critical information and indicators have not become publicly available in solicitations? Ref. AFI 10-701 para. 2.24.7/See Note 8 below. LRAFBI 10-701 para. 2.2.5			
12	Have the OPSEC Coordinators performed an OPSEC Review to examine the unit's measures of performance and to verify unit policies and procedures are in place? Ref. AFI 10-701 para. 5.1/Table 5.1/See Note 9 below.			
13	Have the OPSEC Coordinators conducted a Website Assessment of organizations external-facing web sites to ensure that the unit critical information are not available for exploitation by potential adversaries? Ref. AFI 10-701 para. 5.3.1/See Note 10 below. LRAFBI 10-701 para. 2.4.11			

14	Does the OPSEC Coordinator provide annual training to assigned personnel and maintain a record? LRAFBI 10-701 para. 2.4.9			
15	Has the OPSEC Coordinator maintained a continuity binder (electronic or hard copy) that consists of unit appointment letter, wing or unit CIIL, unit OPSEC Coordinator training certificates, unit initial/annual tracker, and unit policy guidance letter (optional). LRAFBI 10-701 para. 2.4.10			
16	For bulletin boards or OPSEC visual aids that are displayed, is that information current and accurate?			

Notes	
1	Training includes completing OPSEC 1301 (ADLS), AF Identity Mgmt (JKO), Coordinator Face to Face Training (Wg/PM).
2	Coordinators can ensure this by performing walk around spot inspections and checking for critical information left out in the open. Also check for CUI information left uncovered.
3	When developing or reviewing the unit's CIIL, procedures can be developed to ensure that the unit's critical information and indicators are protected from adversary exploitation.
4	Distribute the Unit's critical information and indicators list, memorandums, standard operating procedures, OPSEC Implementation Plans, and HOT TIPS as required.
5	For example: Review and Update the unit CIIL, memorandums, standard operating procedures, and OPSEC Implementation Plans when a new unit commander is assigned or as required.
6	Training should include Tracked Initial OPSEC Training once newly assigned personnel have arrived to the unit. Paragraphs 4.2 - 4.3 also outline training that can be given to unit personnel.
7	If required to do so, the unit OPSEC Coordinator with the help of Public Affairs must review unit documents and photos before they are released to the public to ensure there is no information that could do harm to the unit.
8	If required to do so, the Unit OPSEC Coordinator must review unit contracting documents to ensure that there are no unit CIIL items that could be made available to the public.
9	Examines the unit's measures of performance and verifies that unit policies or procedures are in place.
10	The unit's external-facing websites to include Facebook should be assessed to ensure that its contents do not contain any of the unit's critical information.

Unit OPSEC Public Contracts Checklist				
No.	Question/Reference	Y/N/NA	Remarks	Est Comp.
1	Have contracting representatives who review contracts completed the OPSEC Fundamentals Course within 90 days of appointment of their contracting duties? Ref. AFI 10-701 para 4.4.3			

Unit OPSEC Public Affairs Checklist				
1	Have Public Affairs representatives completed the Air Force Identity Management Course within 90 days of appointment of their public affairs duties? Ref. AFI 10-701 para 4.4.4			