DEPARTMENT OF THE AIR FORCE
DEPUTY CHIEF OF STAFF FOR INTELLIGENCE

AFGM2025-14-406_01
29 AUGUST 2025

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FLDCOMs/FOAs/DRUs

FROM: HQ USAF A2
1700 Air Force Pentagon, Room 4E1070
Washington, DC 20330-1700

SUBJECT: Headquarters Air Force Guidance Memorandum Establishing Proper Use of Commercially Available Information for Air Force Intelligence Missions

References: See annex D.

By Order of the Secretary of the Air Force, this Guidance Memorandum (GM) immediately re-issues the current September 2024 DAFGM 2024-14-01 with changes, as noted, and is an instance of a to-be published Air Force (AF) publication that establishes AF Intelligence policies and procedures to comply with the Intelligence Community (IC) Commercially Available Information (CAI) Policy Framework, reference (a), issued by the Office of the Director of National Intelligence (ODNI) in May 2024. Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other AF publications, the information herein prevails, in accordance with Department of the Air Force Instruction (DAFI) 90-160, *Publications and Forms Management*.

This guidance is applicable to all personnel conducting intelligence or intelligence-related activities, to include civilian employees and uniformed members of the Regular Air Force, the Air Force Reserve, and the Air National Guard, as well as those contractually obligated to comply with Headquarters Air Force (HAF) publications. Air National Guard personnel and units are excluded from this guidance while not in a federalized status supporting an intelligence mission. This publication does not apply to the United States Space Force. Additional policy guidance on the use of CAI within the Department of Defense (DoD) for all cross-functional communities is also expected to be forthcoming.

CAI provides a rapidly growing and fundamentally essential source of information for answering intelligence requirements and information needs for today's data-driven Intelligence missions. However, this data risks unintentional exposure of U.S. persons information (USPI) if used without protections to safeguard privacy and civil liberties. This memorandum reinforces policies meant to protect the USPI and personally identifiable information (PII) of U.S. persons likely available in Sensitive CAI datasets, as defined in Annex C. Additionally, this memorandum designates the Air Force Intelligence Directorate (AF/A2O) as the OPR for CAI Policy, Management, and Reporting.

Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (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. Likewise, ensure that all intelligence and intelligence related activities that require the collection or maintenance of information protected by the Privacy Act of 1974 are authorized by appropriate legal authority, such as a federal statute, EO, or regulation and reference the applicable System of Record Notice(s) (SORN).

This memorandum becomes void after one year has elapsed from the date of this memorandum, or upon publishing of a new publication permanently establishing this guidance, whichever is earlier**.**

MELISSA A. STONE, Brig Gen USAF
Assistant Deputy Chief of Staff for
Intelligence

Attachments:
1. Proper Use of CAI for AF Intelligence Missions
2. Annexes A-D

SUMMARY OF CHANGES

This document has been revised and should be completely reviewed. Changes include incorporation of Privacy Act requirements language, updated publication designation from "DAFGM" to "AFGM" to reflect Air Force-specific scope, clarified and simplified legal review process, streamlined the required due diligence checks, and performed various administrative corrections throughout.

Attachment 1

Proper Use of CAI for AF Intelligence Missions

1. **Overview.**

1.1. In accordance with the IC CAI Policy Framework, reference (a), any units collecting or accessing CAI while conducting intelligence or intelligence-related activities, will:

1.1.1. Ensure CAI collection activities are in support of their authorized intelligence missions with supporting documentation, in accordance with references (a), (b), (c), (d), and (g).

1.1.2. In conjunction with the Office of Primary Responsibility (OPR) for CAI Policy, Management, and Reporting, assess all CAI acquisitions for sensitivity, as outlined in Annex A, in accordance with reference (a).

1.1.3. Ensure access controls are applied, appropriate to the level of sensitivity of the CAI, as outlined in Annex A, in accordance with references (a), (b), (e), and (f).

1.1.4. Collect USPI, including Sensitive CAI, only when the information is reasonably believed to be necessary for the performance of the unit's stated intelligence mission or function, in accordance with references (a) and (b).

1.1.5. Comply with appropriate records keeping standards. For collection of or access to Sensitive CAI, units will document the information required in the CAI utilization process outlined in Annex A, in accordance with references (a), (b), (e), and (f).

1.1.6. Catalogue all CAI acquisitions and licenses within the IC Data Catalogue, at a minimum, in accordance with reference (a).

1.1.7. Share CAI-derived products and non-sensitive, raw CAI data in compliance with established policy guidelines, Foreign Disclosure Offices (FDO) processes, and other applicable Intelligence Community Directives (ICD) and Department of Defense (DoD) policies, in accordance with references (a), (c), (d), (h), (i), (j), (k), (l), and (n).

1.1.8. Limit the sharing of raw Sensitive CAI to those with appropriate mission authorities and an approved utilization agreement, in accordance with reference (a).

1.1.9. Apply strict data security standards for data enclaves used to store, even temporarily, CAI data sets. CAI data determined to be Sensitive CAI will be maintained in systems that implement the appropriate privacy control standards and

achieve authorization to operate (ATO), in accordance with references (a), (c), (m), (o), and (p).

1.1.10. Employ the CAI acquisition agreement process outlined in Annex A , to include reviews by servicing legal offices, civil liberties and privacy offices, and systems security offices, for all new and renewing CAI data acquisitions and licenses in accordance with reference (a).

1.1.11. Employ the utilization agreement process outlined in Annex A to authorize new unit access to existing CAI data acquisitions and licenses and to ensure that CAI data is only used for legitimate intelligence mission purposes using appropriate safeguards and data handling procedures, in accordance with reference (a).

1.2. The Deputy Chief of Staff for Intelligence (AF/A2) designates the Intelligence Directorate (AF/A2O) as the OPR for CAI Policy, Management, and Reporting.

1.3. Units conducting intelligence or intelligence-related activities will have six months from the date of signature of this memorandum to enact policies to comply with this guidance. The authorities to waive wing/unit level requirements in this GM are identified with a Tier ("T-0, T-1, T-2, T-3") number following each compliance statement. See DAFMAN 90-161, Publishing Processes and Procedures, for a description of the authorities associated with the Tier designators. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or to the OPR for non-tiered compliance items.

2. Responsibilities.

2.1. Deputy Chief of Staff for Intelligence (AF/A2) will:

2.1.1. Program funds through the Department of Defense Intelligence Planning, Programming, Budgeting, and Execution (IPPBE) process to support AF CAI requirements. These will include, but are not limited to, the baseline funding to support the acquisition of necessary CAI capabilities, safeguards to protect Sensitive CAI, and approval and oversight mechanisms to perform the tasks outlined in Appendix 2 of this guidance memorandum.

2.1.2. Designate the appropriate staff elements to oversee the management, development, coordination, and implementation of this guidance memorandum.

2.1.3. Provide annual reporting on AF Intelligence access, licensing, and acquisition of Sensitive CAI to DoD and ODNI.

2.2. Director for Intelligence Directorate (AF/A2O) will:

2.2.1. Maintain oversight of and provide guidance for AF Intelligence access, licensing, and acquisition of CAI across the force.

2.2.2. Execute appropriate funds to acquire necessary CAI capabilities; provide mechanisms for rapid analysis, review, and approval of CAI and Sensitive CAI; and establish safeguards to protect Sensitive CAI.

2.2.3. Establish and maintain policies and procedures for implementing the guidance in reference (a).

2.2.4. Implement processes to review and, where appropriate, approve CAI accesses, licensing, and acquisitions to verify 1) elements have the requisite intelligence mission requirements or administrative needs for the data; 2) elements have the legal authority to access or acquire the data; 3) the sensitivity of the data, as per Annex A of this guidance memorandum; 4) the privacy and civil liberties risks associated with the data; 5) the techniques in place to mitigate privacy and civil liberties risks; 6) the data sources, integrity, and quality of the dataset; 7) the security risks associated with the data; and 8) any techniques in place to mitigate security risks.

2.2.4.1. Periodically review assessments annually to ensure that intelligence mission requirements remain current, and safeguards remain sufficient for assessed level of CAI sensitivity.

2.2.5. To the greatest extent feasible, ensure that vendors safeguard queries and other AF information, prohibiting their sharing, selling, transmission, or storage beyond the duration specified in the contract. Furthermore, such information should not be used for any purpose other than auditing.

2.2.5.1. Whenever feasible, request vendors verify that the security of their data repositories meets industry standards, determine who has access to their data repositories, and ensure the repositories are not located in areas subject to inspection or access by key strategic competitors, pacing challenges, or other entities of concern.

2.2.6. Establish and maintain an accessible repository for AF CAI policy, references, and templates.

2.2.7. Within one year of this memorandum, develop guidance pertaining to the auditing of CAI.

2.2.8. Maintain records on all CAI collection, processing, and safeguard measures for one year after the generating intelligence requirement is discontinued or superseded, as per reference (q).

2.2.9. Prepare an annual report on AF intelligence access, licensing, and acquisition of Sensitive CAI for ODNI.

2.2.10. Work with AF Privacy Office to ensure System of Records Notice (SORN) updated to reflect Sensitive CAI accesses, licenses, and acquisitions.

2.3. Commander, Sixteenth Air Force; Commander, National Air and Space Intelligence Center (NASIC); and Major Command (MAJCOM) Commanders will:

2.3.1. Ensure that the access, acquisition, and licensing of CAI in support of intelligence functions are accomplished in accordance with the constraints of this guidance memorandum. **(T-2)**

2.3.2. Communicate CAI requirements for intelligence functions to the AF OPR for CAI Policy, Management, and Reporting, in addition to AF/A2, Air Combat Command (ACC)/ Intelligence Directorate (A2), and NASIC, as appropriate, as outlined in reference (g). **(T-2)**

2.3.3. Coordinate with servicing legal office, Intelligence oversight (IO) office, and civil liberties and privacy office (CLPO) personnel to review authorities, mission requirements, and privacy implications for Sensitive CAI access, licensing, or acquisition. **(T-2)**

2.3.4. Notify, and use as an information resource, the AF OPR for CAI, Policy, Management, and Reporting for the access, licensing, and acquisition of CAI by intelligence elements. **(T-2)**

2.3.4.1. Support the pre-acquisition and pre-utilization analysis of CAI access, licensing, or acquisitions in support of MAJCOM intelligence requirements. **(T-2)**

2.3.5. Store collected Sensitive CAI only on approved networks with an approved ATO and the appropriate privacy control overlay. **(T-2)**

Attachment 2
Annex A

CAI Process

CAI Approval Process. To ensure compliance with this policy, units must complete the following process before acquiring or licensing CAI data, and annually thereafter for Sensitive CAI. Not Sensitive CAI must be reviewed every three years. For Not Sensitive CAI determined to be static, to include books and datasets that have been downloaded onto a USG system without the capacity for changes to the data, periodic review is not required. If collecting USPI or Sensitive CAI, units must also ensure collected CAI meets one of the categories outlined in Procedure 2 of reference (b):

1. Establish authority to access and collect CAI.

    1.1. Verify authority to collect CAI is clearly stated within applicable mission directives, execute orders (EXORDS), or operation orders (OPORDS), and other means of official tasking, such as Requests for Support (RFS).

    1.2. Ensure approved concept of operations (CONOP) exists that characterizes the mission, authorities, intended outcomes, operations execution, and nature of the CAI to be used. See CONOP template in Annex B.

2. Perform sensitivity analysis of the CAI data in question.

    2.1. CAI sensitivity analysis will be performed before acquisition, in coordination with the OPR for CAI Policy, Management, and Reporting in support of acquiring elements.

    2.2. CAI is considered sensitive if the CAI is purchased from a commercial entity through a commercial transaction for a fee or made available by the commercial entity at no cost through a commercial transaction that normally would involve a fee (e.g., a free trial offering of CAI); and the CAI is known or reasonably expected to contain:

        2.2.1. a substantial volume of personally identifiable information (PII) regarding U.S. persons; or

        2.2.2. a greater than de minimis volume of:

            2.2.2.1. sensitive data, which is defined as data that captures personal attributes, conditions, or identifiers that are traceable to one or more specific U.S. persons, either through the dataset itself or by correlating the dataset with other available information; and that concerns the U.S. person's or U.S. persons' race or ethnicity, political opinions, religious beliefs, sexual orientation, gender identity, medical or genetic information, financial data, or any other data the

disclosure of which would have a similar potential to cause substantial harm, embarrassment, inconvenience, or unfairness to the U.S. person or U.S. persons described by the data; or

2.2.2.2. data that captures the sensitive activities of U.S. persons or persons in the United States, with sensitive activities defined as activities that over an extended period of time establish a pattern of life; reveal personal affiliations, preferences, or identifiers; facilitate prediction of future acts; enable targeting activities; reveal the exercise of individual rights and freedoms (including the rights to freedom of speech and of the press, to free exercise of religion, to peaceable assembly—including membership or participation in organizations or associations—and to petition the government); or reveal any other activity the disclosure of which could cause substantial harm, embarrassment, inconvenience, or unfairness to the U.S. person or person in the United States who engaged in the activity.

2.2.2.3. Notwithstanding the above criteria, Sensitive CAI does not include:

2.2.2.3.1. newspapers or other periodicals; weather reports; books, journal articles, or other published works; public filings or records; or similar documents or databases, whether accessed through a subscription or accessible free of cost; or

2.2.2.3.2. limited data samples made available so an IC element can evaluate whether to purchase the full dataset and not accessed, retained, or used for any other purpose unless assessed in accordance with Section II.B of this Policy Framework.

2.3. This sensitivity analysis and the other requirements of this policy only apply to the acquisition and use of CAI materials. The use of publicly available information (PAI) that does not meet the definition of CAI or Sensitive CAI requires management under intelligence oversight policies and safeguards but does not require sensitivity analysis or the special handling safeguards outlined below.

2.4. The AF uses the spectrum model, depicted in figure 1. This model is consistent with the definition of Sensitive CAI above. During sensitivity analysis, analysts will assess the degree of sensitivity as per the Data Sensitivity Analysis template in Annex B. Units should apply the safeguards described in Step 5 below.

Not USPI	Not Sensitive CAI	Moderately Sensitive CAI	Highly Sensitive CAI	Extremely Sensitive CAI
• Does not contain USPI or PII about U.S. Persons	• Negligible amount of USPI or PII about U.S. Persons • Published works • Public social media posts in true name • Public records or filings • Does not include data from within U.S. geographical area	• Moderate amount of USPI or PII about U.S. Persons • Data includes some records from U.S. geographical areas • Public social media posts under associated username • General location data	• Large amount of USPI or PII about U.S. Persons, by percent or absolute #s • Data includes U.S. geographic area • Precise location data • Demographics info	• Primarily contains USPI or PII about U.S. Persons • Data primarily from sources inside the U.S. • Persistent location data • Medical information • Financial data • Biometric data • Data about expressions of guaranteed rights
Safeguards	**Safeguards**	**Safeguards**	**Safeguards**	**Safeguards**

• Basic data handling protocols
• Pre-acquisition CLPO and legal review
• CAI assessment
  • Sourcing, methods, integrity, quality, biases or inferences
• Document to IC Data Catalog
	• Intel oversight Requirements
	• Access restrictions (by organization)
	• Query audits
	• CLPO and legal review every three years
	
	• *Plus earlier safeguards*
		• Pre-use mission and authority review
		• Query limits (policy or technical controls)
		• Annual CLPO and Legal review
		• Filtering, as appropriate
		  • Geographic
		  • Algorithm-based USPI
		  • Full anonymization
		
		• *Plus earlier safeguards*
			• Strict access restrictions (by name)
			• Dissemination controls
			• Pre-dissemination CLPO and legal reviews
			• Written CONOP for approved CAI use
			• Automated masking processes, where feasible
			
			• *Plus earlier safeguards*
				• Query pre-approvals
				
				• *Plus earlier safeguards*

Figure 1 – AF Data Sensitivity Spectrum Model.

2.4.1. Data sensitivity considerations during sensitivity analysis.

2.4.1.1. Amount of USPI or PII about U.S. Persons within the dataset.

2.4.1.1.1. Datasets without any USPI or PII about U.S. Persons are, by definition, not Sensitive CAI.

2.4.1.1.2. Datasets primarily about foreign persons but with negligible amounts of USPI, by volume and percentage, would likely not be Sensitive CAI but would still require appropriate marking, retention, and dissemination controls under Intelligence Oversight program guidelines.

2.4.1.1.3. Datasets may be characterized as Moderately Sensitive, Highly Sensitive, or Extremely Sensitive depending on the absolute volume, type, or percentage of USPI or PII about U.S. Persons in the dataset.

2.4.1.1.4. Datasets primarily composed of USPI or PII about U.S. Persons, or including protected data types such as protected health information (PHI), financial records, or private demographics data, are always characterized as Extremely Sensitive.

2.4.1.2. Type of USPI or PII about U.S. Persons within the dataset.

2.4.1.2.1. USPI that would not meet the definition of PII would typically be considered less sensitive than other forms of sensitive data.

2.4.1.2.2. Personally or professionally published material, such as published works, social media posts published in true name without privacy controls, or public records and filings, should not be characterized as Sensitive CAI, but would still require safeguards under intelligence oversight policy.

2.4.1.2.2.1. PAI that does not meet the definition of CAI, including public and freely available posts by commercial entities, should be handled in accordance with intelligence oversight policy requirement but does not require any special handling under this memorandum.

2.4.1.2.3. Commercially purchased material published or posted in social media anonymously or under a username, when tied to original creators, would be characterized as Moderately Sensitive or Highly Sensitive, depending on the nature of the information posted.

2.4.1.3. Datasets that do not include U.S. geographic locations or prefilter to remove U.S. geographic locations would be characterized as Not USPI, Not Sensitive, or Moderately Sensitive, depending on the other factors considered.

2.4.1.3.1. Datasets that include only general location data within the U.S. would be considered Moderately Sensitive while datasets that offer precise location data would be considered Highly Sensitive. Datasets that offer persistent location data within the U.S. would be characterized as Extremely Sensitive.

2.4.1.4. Datasets that present significant demographics information about U.S. persons would always be characterized as Highly Sensitive, at a minimum. Demographics information includes, but is not limited to, sex, race, age, religion, and registered political parties.

2.4.1.4.1. Information that would depict associations, political opinions, gender identities, sexual orientation, or other personal information that could raise cause for discrimination or adverse public opinion about a U.S. Person would always be characterized as Extremely Sensitive.

2.4.1.4.2. Datasets which present pattern of life information, data about the exercise of constitutionally protected rights by U.S. persons, U.S. persons' private financial records, medical or genetic information of U.S.

persons, or biometric data about U.S. persons, would be characterized as Extremely Sensitive.

2.5. While sensitivity analysis is mission, directorate, and unit specific, new units or directorates requesting access to existing datasets should accept existing sensitivity analysis unless specific mission parameters necessitate a review.

2.6. Data purchased prior to the issuance of this memorandum will require a sensitivity analysis to be completed within one year, unless excepted in writing by the AF OPR for CAI Policy, Management, and Reporting.

3. Complete Pre-Acquisition or Pre-Utilization Assessment

3.1. Prior to acquisition of CAI, units must notify and coordinate with the AF OPR for CAI Policy, Management, and Reporting to complete the following pre-acquisition assessment checklist items. Units can delegate in writing the approval and signature of pre-acquisition checklists to the O5 or squadron commander level for Sensitive CAI sources and to any appropriate level for CAI sources deemed not to contain Sensitive CAI.

3.1.1. If exigent circumstances exist to allow for acquisition of CAI without following the below procedures, units will document those circumstances in a memorandum signed by the first GO-level officer, or officially delegated O6, in their chain of command. Exigency generally requires an immediate need to acquire, access, or collect information when circumstances do not allow for the time it takes to follow the procedures outlined in this memorandum. See Exigent Circumstances template in Annex B.

3.1.1.1. Units will complete the procedures outlined below promptly after collection or access.

3.1.1.2. All activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States, applicable executive orders, and DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities,* 8 Aug 2016.

3.1.2. Perform a source assessment of the CAI vendor.

3.1.2.1. For traditionally published works, determine to the maximum amount feasible:

3.1.2.1.1. The publication's authenticity and veracity.

3.1.2.2. For all other types of CAI, use the Pre-Acquisition Questionnaire template in Annex B to determine to the maximum extent feasible:

3.1.2.2.1. The original sources of vendor data, as feasible, depending on the nature of the AF relationship with the vendor and the security requirements of the contract.

3.1.2.2.2. How the vendor collects, aggregates, processes, enhances, and makes available the data in their data sets.

3.1.2.2.3. The integrity and quality of their CAI, to include underlying biases or inferences and consistency with standards for accuracy and objectivity, with a focus on the reliability of the information.

3.1.2.2.4. Vendor ability to apply geographic, USPI, or other applicable prefiltering.

3.1.2.2.5. Vendor confidentiality standards, to include safeguarding of queries, data accesses, and download records.

3.1.2.2.6. Security, operational, and counterintelligence risks associated with accessing or collecting any Sensitive CAI from the vendor, along with steps to mitigate those risks, to include which other IC elements could be using the same vendor to access the same data, creating a pattern of use that may expose operational imperatives.

3.1.3. For sensitive CAI, perform due diligence checks on vendors and vendor processes, sources, and associated personnel to ensure that vendor is not engaged in activities that could cause damage to the credibility of the AF with the public or allies. Information from the Pre-Acquisition Questionnaire template in Annex B may provide some of this information, but units should leverage existing Department of the Air Force and DoD capabilities to perform due diligence activities when possible. This includes checks that:

3.1.3.1. Vendor has not been banned from operating in any part of the U.S., U.S. Territories, NATO ally countries, or FVEY partner territories; and

3.1.3.2. Vendor does not have a pattern of export law violations, substantiated violations of U.S. privacy and civil liberties statues or laws, relevant legal challenges in U.S. courts, or restrictions from use or operations within the U.S. or its territories. Negative press does not equate to an unfavorable situation.

3.1.3.3. Due diligence checks will be performed annually. If units become aware of information that could make the continued use of unfavorable to the AF, they will coordinate with IO, CLPO, legal, and higher echelons as required to adjudicate continued use of the vendor or product.

3.1.4. Where the nature of the contractual relationship with the vendor and the security requirements of the contract allows, ensure contracts specify that:

3.1.4.1. Queries will not be shared, sold, transmitted, stored for longer than the duration of the contract states, or used for any other purpose beyond that of auditing; and

3.1.4.2. Vendors will verify that the security of their data repositories meet industry standards and are not located in areas subject to inspection or access by key strategic competitors, pacing challenges, or other entities of concern. See Pre-Acquisition Questionnaire template in Annex B.

3.1.5. Obtain a legal review from the servicing legal office. See Pre-Acquisition Approval Memorandum template in Annex B.

3.1.6. For Sensitive CAI, complete a CLPO and IO officer review from servicing offices to ensure adequate unit safeguards for level of assessed data sensitivity. See Pre-Acquisition Approval Memorandum template in Annex B.

3.1.7. Perform a systems security review to ensure data repositories owned or operated by the Air Force meet required security standards to safeguard PII and Sensitive CAI. See Pre-Acquisition Approval Memorandum template in Annex B.

3.2. After acquisition of CAI, additional units that wish to gain access to the data set must have completed the following pre-utilization assessment checklist items at the unit and not the individual level. Units can delegate in writing the approval and signature of pre-utilization checklists to the O5 or squadron commander level for Sensitive CAI sources and to any appropriate level for CAI sources deemed not to contain Sensitive CAI. See Pre-Utilization Approval Memorandum template in Annex B.

3.2.1. Review the vendor source assessment performed prior to acquisition.

3.2.2. Obtain a legal review from the servicing legal office.

3.2.3. When Sensitive CAI is present, complete a CLPO and IO review to ensure adequate safeguards for the assessed level of data sensitivity. CLPO and IO elements are expected to review administrative controls while offering advice on necessary technical controls.

3.2.4. Perform a systems security review to ensure data repositories meet required security standards to safeguard PII and Sensitive CAI.

4. Prepare annual report to the Office of the Director of National Intelligence (ODNI) of all Sensitive CAI holdings, collections, and accesses.

4.1. AF OPR for CAI Policy, Management, and Reporting will prepare the report using the template provided by ODNI.

4.1.1. At a minimum this report will include:

4.1.1.1. the purpose of the access, collection, or processing, and intended uses of the Sensitive CAI;

4.1.1.2. the nature or characterization, and volume, of the Sensitive CAI access or collection;

4.1.1.3. authority under which the Sensitive CAI is accessed, collected, or processed;

4.1.1.4. the source of the Sensitive CAI and from whom the Sensitive CAI was accessed or collected;

4.1.1.5. the mechanics of the access, collection, and processing the Sensitive CAI;

4.1.1.6. offices which participated in the acquisition process, conduced the source assessment, and approved the acquisition;

4.1.1.7. if applicable, the basis for relying on the exigent circumstances exception;

4.1.1.8. the policies and procedures for safeguarding the Sensitive CAI;

4.1.1.9. whether the vendor has made unevaluated data or information available to any other IC elements or foreign partners and, if so, which elements or partners; and

4.1.1.10. any licensing agreements, terms of agreement, or contract restrictions applicable to the Sensitive CAI.

4.1.2. Document CAI collection within the IC Data Catalog.

5. Safeguard access to CAI.

5.1. Safeguarding access to CAI will incorporate both technical and administrative controls to ensure the appropriate level of safeguards as data sensitivity increases. Some types and categories of data may have additional safeguards that are already directed by other policies, statutes, security classification guides (SCGs), and instructions. Data owners will establish specific details of the necessary safeguards based on the assessed level of sensitivity, but based on the proposed measures outlined below.

5.1.1. All CAI, including CAI determined to be Not USPI will apply at a minimum the following safeguards:

5.1.1.1. Apply basic data handling protocols.

5.1.1.2. Complete source assessment, as per Step 3.

5.1.1.3. Classify collected CAI in accordance with an applicable security classification guide (SCG).

5.1.1.3.1. Many forms of data may be unclassified when collected or purchased, however depending on the organization's SCG and authorities under which the CAI is collected the classification and dissemination or sharing restriction may vary greatly.

5.1.1.4. Apply normal dissemination controls in accordance with classification guidance and FDO process.

5.1.2. CAI determined not to be Sensitive CAI while still containing USPI or PII about U.S. Persons will apply at a minimum the safeguards outlined in 5.1.1. In addition to those safeguards, the following safeguards will also apply:

5.1.2.1. Abide by USPI and information marking requirements.

5.1.2.2. Apply appropriate data repository security controls, including the requirement for a privacy overlay for PII and PHI outlined in NIST SP 800-53 and current ATO.

5.1.2.3. Develop and maintain a CONOP for approved CAI use. These CONOPs can be organic to the unit or specify supporting units CONOP.

5.1.2.4. Restrict access to data by organization and mission, to include controls on raw data sharing and a unit-level pre-dissemination review for USPI.

5.1.2.5. Perform audits on queries and access in accordance with the type and sensitivity of the CAI being used.

5.1.2.6. Servicing CLPO, IO and legal offices conduct a periodic review every three years. See Annual Review Approval Memorandum template in Annex B.

5.1.2.6.1. For Not Sensitive CAI determined to be static, periodic review is not required. This can include books, periodicals, and other published works that are not updated, as well as datasets that are downloaded onto a USG system without further updates. The determination that CAI is static will be made by the acquiring unit.

5.1.3. CAI determined to be Moderately Sensitive will apply at a minimum the safeguards outlined in 5.1.1. and 5.1.2. In addition to those safeguards, the following safeguards will also apply:

5.1.3.1. Conduct a pre-use mission and authority review, as per Step 3.

5.1.3.2. Apply administrative or technical controls on queries that users can perform.

5.1.3.3. Employ filtering, on vendor systems or at a processing stage between the data repository and the user interface. Filters can include:

5.1.3.3.1. geographic filters to prevent searches or data returns within the US and its territories;

5.1.3.3.2. algorithm-based USPI filters; or

5.1.3.3.3. full anonymization to mask all PII unless units request specific individual's records be demasked.

5.1.4. CAI determined to be Highly Sensitive will apply at a minimum the safeguards outlined in 5.1.1., 5.1.2., and 5.1.3. In addition to those safeguards, the following safeguards will also apply:

5.1.4.1. Vendor must abide by confidentiality standards set forth in 3.1.4.1.

5.1.4.2. Pre-dissemination CLPO, IO, or legal reviews, as required for the specific Sensitive CAI.

5.1.4.3. Automated masking processes, where feasible.

5.1.4.4. Strict, individual access restrictions based on zero-trust security standards, when feasible.

5.1.5. CAI Determined Extremely Sensitive will apply at a minimum the safeguards outlined in 5.1.1., 5.1.2., 5.1.3, and 5.1.4. In addition to those safeguards, the following safeguards will also apply:

5.1.5.1. Establish process for query pre-approvals, signed the first available O6/GG15 within the chain of command. See Query Pre-approval Memorandum template in Annex B.

5.1.5.1.1. Approved queries can be multiple use for the authorized time duration; however, but the same query nexus or key words must be used.

5.1.5.1.2. Queries must be specific in nature to minimize excess collection on USPI.

6. Records Management Requirements

6.1. Units should have in place procedures that require data management planning from the point of access or collection, throughout the data lifecycle, to disposition, in accordance with reference (b) and instructions in AFI 33-322, *Records Management Program*, 4 Jun 2012 and the Records Disposition Schedule (RDS) published at https://www.my.af.mil/afrims/afrims/afrims/rims.cfm.

6.2. The AF OPR for CAI Policy, Management, and Reporting will ensure that AF Systems of Records Notices (SORNs) are updated to reflect the Sensitive CAI holdings or accesses available to the AF.

7. Disputes

7.1. Disputes in the handling of CAI sensitivity analysis during the approval processes will be adjudicated by the AF OPR for CAI Policy, Management, and Reporting or the next higher office in the chain of command.

7.1.1. Disputes in the legal, CLPO, IO, or security office review will be adjudicated through the legal, CLPO, IO, or security channels respectively.

7.2. Violations of these procedures, handling requirements, or the safeguard processes outlined for all CAI and Sensitive CAI will be treated and investigated as a questionable intelligence activity (QIA).

Annex B

Templates

CONOP (Memorandum Format) Template

[Letterhead]

DATE

(U) CONCEPT OF OPERATIONS: UNIT and ACTIVITY

FROM: Unit
Address
City, State, Zip Code

References: (a) DoDD 3115.18, DoD Access to and Use of Publicly Available Information (PAI)
(b) DoDI 3115.12, Open Source Intelligence (OSINT)
(c) IC Policy Framework for Commercially Available Information (CAI)
(d) DoDM 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities
(e) AFI 14-404, Oversight of Intelligence Activities
(f) AFMAN 14-405, Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR)
(g) [Mission Directive]
(h) [all other applicable references]

1. (U) Situation
    1. [Give brief introduction or overview.]

    2. (U) Mission.
        a. [Mission Statement]
        b. [Authorities (including authority to collect PAI and CAI)]
        c. [Intended Results or Outcomes]

    3. (U) Execution
        a. [Who, What, When, Where, How]
        b. [Safeguards (must correlate to requested level of Sensitive CAI required for mission.)]
        c. [Resourcing including Manning, Funding, Equipment, Training]
        d. [Methodology]
        e. [Dissemination (including all dissemination controls required for release according to sensitivity of CAI requested for mission)]

4. (U) Administration and Logistics

    a. [All applicable reviews and approval dates (reviews should be annexes as req and the body just needs to list type of review, reviewer/approver/DTG)]
    b. [Ensure files are properly marked (ICD 206 and DoDM 5240.01, Procs. 3 and 4)]
    c. [Auditing procedures and due diligence measures]
    d. [Report questionable intelligence activities using procedures in AFI 14-104]

5. [(U) CAI or Sensitive CAI (remove if no CAI or Sensitive CAI)
    a. Type, Vendor, Acquisition Date, contract number, terms of use, if known
    b. Data Sources
    c. Storage
    d. Access
    e. IC Catalog nomenclature
    f. Dissemination controls
    g. Approval Checklist of Use of Sensitive CAI
    h. Sensitivity Analysis Results including Reviewer/Approver and DTG]

6. (U) Command and Control
    a. [Command and Control Plan]

7. (U) Point of contact for this CONOP is [POC].

Signature Block

CONOP (PowerPoint Format) Template

(CUI) Mission Statement: Conduct OSINT Activities to Monitor and Track Vessel and Aircraft Movement in the Bering Strait

Authorities

16 AF Delegation of OSINT Authorities Memorandum, 2024

INDOPACOM OPORD XXXX Annex XXXX

EXORD XXXXXX

Place all authorities, OPORDS, EXORDS, or CONOPS the activity will be authorized under in this section. For exercises this may be OT&E

Include mission analysis results correlating to requested level of sensitive CAI for use, including DTG and approver.

Exigent Circumstances, including DTG + approver

Intelligence or Operational Requirements

PIR 1, 4,7 & 8

DIA XXXXXXX

NAVXXXXXXX

AFXXXXXXXXX

For most Sensitive Categories of CAI annotate applicable circumstance per DoDM 5240.01 section 3

List all requirements the activities outlined in this CONOP are intended to meet. For PAI-R this may include MOE(S) in additional to specific operational goals such as Situational Awareness, Sentiment Analysis, or OPSEC

(CUI) OPERATIONAL CONCEPT : Conduct OSINT Activities to Monitor and Track vessel and aircraft movement in the Bering Strait

(U) 5 W's

(U) Who: 123 AOC

(U) What: Conduct OSINT Activities to Monitor and Track vessel and aircraft movement in the Bering Strait

(U) Why: The Bering Strait is a critical Sea Line of Communication separating Asia from North America. Its narrowest point is only 82 miles across, separating Alaska from Russia.

(U) When: 01 FEB 2020 – thru 01 FEB 2021

(U) Where: Outpost Grizzly, Yukon AK

(CUI) How: Use CAI subscriptions to depict real time aircraft and vessel movements including, geolocation, speed, heading, tail or vessel number and nationality of registration and operation

(U) Resourcing

(U) Manning – What are the personnel and duty positions required to man this CONOP. This is not C2, but the executors of this operation

(U) Equipment Requirements (include technology, space, communication equipment, CAI data purchases, MA

(U) Funding (Cost Estimate, Funding Source – include applicable LOA, Funding type O&M, COPE, MIP, NIP, Training)

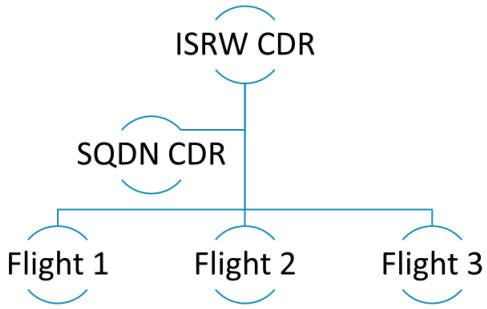
(U) Training (Include training required to meet operational requirements, either past or future and any associated costs)

SENSITIVE CAI CHECKLIST

Sensitive CAI Checklist	Approvers	Signature
Sensitivity Analysis	SQDN CDR or approval level as req	_____
Mission Analysis and Review	SQDN CDR or approval level as req.	_____
Safeguards Assessment and Review	SQDN CDR or approval level as req	_____
Legal Assessment and Review	JAO	_____
CLPP Assessment and Review	Civil Liberties and Privacy Office	_____
I/O Assessment and Review	Intelligence Oversight	_____
Security Assessment and Review	SSO	_____
Counter-intelligence Review	OSI Field Office	_____

COMMAND and CONTROL

C2: Outline your C2 in this block, may be written or graphic presentation. This may change on the level of sensitivity of the CAI, partners, GCC coordination and approval requirements, OPORDS, and tasking or if exigent circumstances are involved.



COORDINATION/ CONOP APPROVERS : This will change based on your own organization hierarchy, sensitivity of CONOP and supported mission, for NGB units you may need additional approvals from state or NGB depending on activity

Coordination Checklist and Approvers

- ☐ **Squadron Commander**
- ☐ **Wing Commander**
- ☐ **TBD**
- ☐ **TBD**

Data Sensitivity Analysis Template

[Letterhead]

DATE

MEMORANDOM FOR RECORD

FROM: ORG/SYMBOL
Organization
Street Address
City ST 12345-6789

SUBJECT: CAI Sensitivity Assessment of (Source)

References: (a) DoDD 3115.18, DoD Access to and Use of Publicly Available Information (PAI)
(b) DoDI 3115.12, Open Source Intelligence (OSINT)
(c) IC Policy Framework for Commercially Available Information (CAI)
(d) DoDM 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities
(e) AFI 14-404, Oversight of Intelligence Activities
(f) AFMAN 14-405, Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR)
(g) DoDD 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense
(h) DIA Open Source Intelligence Security Classification Guide 31 May 2022.
(i) Proper Use of Commercially Available Information (CAI) and Sensitive CAI for AF Intelligence Missions, DATE, Annex A Sensitive CAI Spectrum Model

1. CAI SENSITIVY ASSESSMENT Process. The below process is intended to provide a score sheet to determine the appropriate level of safeguards required to protect U.S. persons Information (USPI) and Personally Identifiable Information (PII) about U.S. persons in accordance with reference (i). The safeguards required to work with the below assessed data source will correlate to the highest rating on the matrix. For example, any assessed Medical or Biometric information in a dataset would be categorized as Extremely Sensitive, even if there is no minimal USPI Medical or biometric data would still be categorized as extremely sensitive per annex XXXXX and require the corresponding safeguards.

2. Assess the precision of locational data about U.S. persons present or potentially present in the commercial tool or dataset. Locational data includes anything that provides data or viewable metadata about the location of a device or individual, the origin of a social media post or other

activity, or any other material that could provide information about the pattern of life of a U.S. person.

Factors	Not USPI	Not Sensitive CAI	Moderately Sensitive CAI	Highly Sensitive CAI	Extremely Sensitive CAI
Location Data	□ None	□ Filtered to remove U.S. geographic area	□ General location, accuracy to more than 1000 meters	□ Precise, but not persistent location, accuracy to less than 1000 meters	□ Precise, persistent location of USPERS

3. Assess the source of the data, to include personal electronic devices, social media services, or another electronic database, present within the commercial tool or dataset.

Factors	Not USPI	Not Sensitive CAI	Moderately Sensitive CAI	Highly Sensitive CAI	Extremely Sensitive CAI
Source devices or services		□ No data from sources or devices within the U.S. geographic area	□ Includes some data from sources or devices within the U.S. geographic area	□ Includes a large amount of data from sources or devices within the U.S. geographic area, along with foreign locales	□ Data primarily from sources or devices within the U.S. geographic area

4. Assess the degree of information about social media posts of U.S. persons present or potentially present in the commercial tool or dataset.

Factors	Not USPI	Not Sensitive CAI	Moderately Sensitive CAI	Highly Sensitive CAI	Extremely Sensitive CAI
Public Social media activities	□ None	□ Public posts in true name	□ Public posts under username (if associated to true name)	□ Dataset extracts demographic info from public posts	□ Dataset extracts details about exercise of protected rights from public posts

5. Assess the type, percentage, or absolute volume of sensitive data, to include USPI and PII, about U.S. persons present or potentially present in the commercial tool or dataset.

Factors	Not USPI	Not Sensitive CAI	Moderately Sensitive CAI	Highly Sensitive CAI	Extremely Sensitive CAI
Type of sensitive data	□ None	□ Published works □ Public filings or records		□ General demographic info (sex, race, age, religion, registered party, etc.) □ Associations or memberships in organizations that would not likely result in discrimination or adverse public opinion	□ Medical info □ Financial info □ Biometric info □ Demonstrates expressions of guaranteed rights □ Associations, political opinions, gender identities, sexual orientations, or other personal information that may result in discrimination or adverse public opinion
Percentage of sensitive data	□ None	□ Filtered to remove USPI □ Incidental amt of PII (<1% of data)	□ Moderate amt of PII (<5% of data)	□ Large amt of PII (<50% of data)	□ Primarily PII (>50% of data)
Volume of sensitive data	□ None	□ Negligible # of USPERS (<5000 individuals)	□ Moderate # of USPERS (<50,000 individuals)	□ Large # of USPERS (<1,000,000 individuals)	□ Very large # of USPERS (>1,000,000 individuals)

Pre-Acquisition Questionnaire

[Letterhead]

SUBJECT: USAF Commercially Available Information Vendor Questionnaire

1. Purpose. This questionnaire will assist the Air Force (AF) in determining if potential tools will meet IC, DoD, and AF PAI/CAI auditing and safeguarding requirements.

2. QUESTIONS:

a. Are members of your company involved with this contract willing and able to sign a non-disclosure agreement (NDA)?

b. By what methods are your data collected, generated, or aggregated?

c. What standard or proprietary processing steps and enhancements do you apply against that data?

d. By what modalities will you make that data available to customers?

e. Does your tool provide an auditing capability?

(1) If so, how in depth are your audits? (i.e. do they include search terms, times of searches, geolocations, etc)

(2) Is the customer able to audit the usage or is the audit provided by the vendor?

(3) How are results of the audits provided to the USG?

f. Does your tool allow for USPI or geographic filtering?

(1) If so, how does your tool filter out USPI?

(2) Are you able to block search results from specific geographic areas?

(3) Can admins turn on or off these filters by individual account?

g. What policies do you have in place for compliance with GDPR and CCPA?

h. Does the vendor retain access to our search queries?

(1) If so, who in the company has access to the search queries? If not, how are queries deleted?

(2) For how long are search queries stored?

(3) Where are the queries stored and what security measures do you have in place?

(4) Do the individuals in your company who have access to the queries maintain a security clearance?

(5) Are there any foreign nationals who have access to the queries?

i. Where are your data servers located?

j. Does your company sell its user data to any third-party entities?

k. Do you sell or share data with any foreign entities?

l. Where are your secure enclaves physically located?

m. Is your company owned by or have significant shareholders (greater than 25%) that are foreign nationals? If so what countries and citizenships?

n. Is your company currently involved in any legal proceedings with the USG?

o. Is your product banned anywhere in the US or its territories? If so, why?

p. Is your product banned within the European Union or the United Kingdom, Australia, New Zealand, or Canada? If so where and for what reason?

q. Has your tool been previously vetted or used by any other DoD entity?

(1) If yes, who and when?

Pre-Acquisition Approval Memorandum Template

[Letterhead]

DATE

MEMORANDOM FOR AF/A2O
ATTENTION: OPR, CAI POLICY, MNGMNT, AND REPORTING

FROM: ORG/SYMBOL
Organization
Street Address
City ST 12345-6789

SUBJECT: Approval Review for Acquisition of [Sensitive/Non-Sensitive] Commercially Available Information (CAI) from [Source]

References: (a) IC Policy Framework for Commercially Available Information (CAI)
(b) Memorandum Proper Use of Commercially Available Information (CAI) and Sensitive CAI for AF Intelligence Missions.

1. Purpose. This approval checklist documents the signatures and approvals required to complete the acquisition of [source] which contains [dynamic/static] CAI determined to be [Not U.S. Persons Information (USPI)/Not Sensitive/ Moderately Sensitive/Highly Sensitive/Extremely Sensitive].

2. This document should be maintained with annual recertifications for the duration the contract plus five (5) years, the duration of access or retention of the CAI plus five (5) years, or five years, whichever is longer.

3. The below pre-acquisition review steps have been completed for [Source]:

a. Mission and authorities' analysis: [Date completed, Point of Contact, POC email]

[Signature block]

b. Pre-acquisition questionnaire (if applicable): [Date completed, Point of Contact, POC email]

[Signature block]

c. Sensitivity analysis: [Date completed, Point of Contact, POC email]

[Signature block]

d. Legal Review: [Date completed, Point of Contact, POC email]

[Signature block]

e. Civil Liberties and Privacy Office Review: [Date completed, Point of Contact, POC email]

[Signature block]

f. Intelligence Oversight Review: [Date completed, Point of Contact, POC email]

[Signature block]

g. Systems Security Office Review: [Date completed, Point of Contact, POC email]

[Signature block]

4. This CAI is [Approved/disapproved] for acquisition, [use, dissemination, sharing, or retention].

5. Point of Contact for the memorandum is [POC].

Signature Block

Pre-Utilization Approval Memorandum Template

[Letterhead]

DATE

MEMORANDOM FOR AF/A2O
ATTENTION: OPR, CAI POLICY, MNGMNT, AND REPORTING

FROM: ORG/SYMBOL
Organization
Street Address
City ST 12345-6789

SUBJECT: Approval Review for Utilization of [Sensitive/Non-Sensitive] Commercially Available Information (CAI) from [Source] by [Unit]

References: (a) IC Policy Framework for Commercially Available Information (CAI)
(b) Memorandum Proper Use of Commercially Available Information (CAI) and Sensitive CAI for AF Intelligence Missions.

1. Purpose. This approval checklist documents the signatures and approvals required to approve [unit's] use of [source] which contains CAI determined to be [Not U.S. Persons Information (USPI)/Not Sensitive/ Moderately Sensitive/Highly Sensitive/Extremely Sensitive].

2. This document should be maintained with annual recertifications for the duration of the unit's access or retention of the CAI plus five (5) years.

3. The below pre-utilization review steps have been completed:

a. Mission and authorities' analysis: [Date completed, Point of Contact, POC email]

[Signature block]

b. Sensitivity analysis: [Date completed, Point of Contact, POC email]

[Signature block]

c. Legal Review: [Date completed, Point of Contact, POC email]

[Signature block]

d. Civil Liberties and Privacy Office Review: [Date completed, Point of Contact, POC email]

[Signature block]

e. Intelligence Oversight Review: [Date completed, Point of Contact, POC email]

[Signature block]

f. Systems Security Office Review: [Date completed, Point of Contact, POC email]

[Signature block]

4. This CAI is [Approved/disapproved] for acquisition, [use, dissemination, sharing, or retention].

5. Point of Contact for the memorandum is [POC].

Signature Block

Periodic Review Approval Memorandum Template

[Letterhead]

DATE

MEMORANDOM FOR AF/A2O
ATTENTION: OPR, CAI POLICY, MNGMNT, AND REPORTING

FROM: ORG/SYMBOL
Organization
Street Address
City ST 12345-6789

SUBJECT: Periodic Review of [Sensitive/Non-Sensitive] Commercially Available Information (CAI) from [Source]

References: (a) IC Policy Framework for Commercially Available Information (CAI)
(b) Memorandum Proper Use of Commercially Available Information (CAI) and Sensitive CAI for AF Intelligence Missions.

1. Purpose. This review checklist documents the signatures and approvals required for [source] which contains CAI determined to be [Not U.S. Persons Information (USPI)/Not Sensitive/ Moderately Sensitive/Highly Sensitive/Extremely Sensitive].

2. This document should be maintained for five years.

3. The below annual review steps have been completed for [Unit] use of [Source]:

a. Mission and authorities' analysis: [Date completed, Point of Contact, POC email]

[Signature block]

b. Sensitivity analysis: [Date completed, Point of Contact, POC email]

[Signature block]

c. Legal Review: [Date completed, Point of Contact, POC email]

[Signature block]

d. Civil Liberties and Privacy Office Review: [Date completed, Point of Contact, POC email]

[Signature block]

e. Intelligence Oversight Review: [Date completed, Point of Contact, POC email]

[Signature block]

f. Security Office Review: [Date completed, Point of Contact, POC email]

[Signature block]

4. This CAI is [Approved/disapproved] for continued use by [unit].

5. Point of Contact for the memorandum is [POC].

Signature Block

Exigent Circumstances Approval Memorandum Template

[Letterhead]

DATE

MEMORANDOM FOR AF/A2O
ATTENTION: OPR, CAI POLICY, MNGMNT, AND REPORTING

FROM: ORG/SYMBOL
Organization
Street Address
City ST 12345-6789

SUBJECT: Approval of Exigent Circumstances Collection of Commercially Available Information (CAI)

References: (a) IC Policy Framework for Commercially Available Information (CAI)
(b) Memorandum Proper Use of Commercially Available Information (CAI) and Sensitive CAI for AF Intelligence Missions.
(c) DoD Manual (DoDM) 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 8 Aug 2016

1. Purpose. I hereby approve the immediate [acquisition/access/collection] of [source]. While this source may contain CAI, exigent circumstances require that we collect this information in a timely manner.

2. Justification. [Document the reasons for collecting under exigent circumstances.]

3. [Unit] will complete the appropriate Approval checklist [document the expected timeframe].

4. Point of Contact for the memorandum is [POC].

Signature Block

Query Pre-approval Memorandum Template

[Letterhead]

DATE

MEMORANDOM FOR RECORD

FROM: ORG/SYMBOL
Organization
Street Address
City ST 12345-6789

SUBJECT: Approval of Query for Extremely Sensitive Commercially Available Information (CAI) on [Subject/Name/Location/Named Area of Interest/Organization]

References: (a) IC Policy Framework for Commercially Available Information (CAI)
(b) Memorandum Proper Use of Commercially Available Information (CAI) and Sensitive CAI for AF Intelligence Missions.

1. Request Approval for Extremely Sensitive CAI Query on [specific details, to include name, identifying information as applicable, address, associated organizations/business that you intend the query to encompass.] This query may generate incidental results of Sensitive CAI about [details] due to the nature of the search [remove this sentence if not needed. Note: All CAI queries on NAI(s), bulk searches, or using a geo-fence (non-pinpoint) located within the United States and its territories will be considered an Extremely Sensitive CAI query.]

a. (Example) Request Approval for Extremely Sensitive CAI Query on The Chinese Business Council of Houston, TX, 1234 ABC Drive, 12345, phone number XXX-XXXX, owner John/Jane Doe. This query may generate incidental results collection of Sensitive CAI about other U.S. Persons in the Houston, TX area located near this address due to the nature of the search.

2. Justification. [At a minimum this must include mission supported and corresponding CONOP, intelligence, or operational requirements this query may answer, and impacts to mission if this query is not approved. The CONOP, including DTG approved, must be noted in this section. Pre-acquisition or pre-utilization approval memorandum should be noted as well. If there is no corresponding CONOP and pre-acquisition or pre-utilization approval memorandum, the following sub bullets must be completed.]

a. Legal Review (DTG and approving authority)

b. CLPO Review (DTG and approving authority)

c. Security Review (DTG and approving authority)

d. Intelligence Oversight Review (DTG and approving authority)

3. Safeguards. [This area will describe the safeguards and control measures that will be used to protect the information, including incidental results.]

4. Point of Contact for the memorandum is [POC].

Signature Block

5. Approving Authority and Disposition. This Sensitive CAI query is [approved/disapproved].

Signature Block (O6/GG15 approver)

Annex C

Abbreviations

ATO	authorization to operate
CAI	commercially available information
CLPO	civil liberties and privacy office
CONOP	concept of operations
EXORD	execute orders
IO	intelligence oversight
IPPBE	Intelligence Planning, Programming, Budgeting, and Execution
NDA	non-disclosure agreement
ODNI	Office of the Director of National Intelligence
OPORD	operation order
OPR	office of primary responsibility
OSINT	open source intelligence
PAI	publicly available information
PHI	protected health information
PII	personally identifiable information
QIA	questionable intelligence activity
RDS	Records Disposition Schedule
RFS	Request for Support
SORN	System of Records Notice
USPERS	U.S. Persons
USPI	U.S. Persons information

Glossary

access The viewing or examining of information for official purposes, or establishing the capability to view or examine information for official purposes (e.g., by purchasing a license), where the information viewed or examined is not stored or otherwise maintained under the control of the IC element.
(*ODNI Intelligence Community Policy Framework for CAI*, May 2024)

acquisition The acquiring by contract with appropriated funds of supplies or services by and for the use of the Federal Government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated.
(Federal Acquisition Regulation)

ATO The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.
(OMB Circular A-130, *Managing Information as a Strategic Resource*, 28 Jul 2016)

CAI Any data or other information that is of a type customarily made available or obtainable and sold, leased, or licensed to members of the general public or to non-governmental entities for purposes other than governmental purposes. CAI also includes data and information for exclusive government use knowingly and voluntarily provided by, procured from, or made accessible by corporate entities at the request of a government entity or on their own initiative.
(*ODNI Intelligence Community Policy Framework for CAI*, May 2024)

collection — Information is collected when it is received by a Defense Intelligence Component, whether or not it is retained by the Component for intelligence or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to the Component. Collected information does not include:

• Information that only momentarily passes through a computer system of the Component;

• Information on the Internet or in an electronic forum or repository outside the Component that is simply viewed or accessed by a Component employee but is not copied, saved, supplemented, or used in some manner;

• Information disseminated by other Components or elements of the Intelligence Community; or

• Information that is maintained on behalf of another U.S. Government agency and to which the Component does not have access for intelligence purposes.
(DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 8 Aug 2016)

PAI — Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public.
(DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 8 Aug 2016)

pattern of life — The specific set of behaviors and movements associated with a particular entity over a given period of time.
(Activity Based Intelligence Reference Aid, 1 Mar 2016)

PHI "Individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. "Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.
(Health Insurance Portability and Accountability Act of 1996 [HIPAA], Public Law 104-191, 21 Aug 1996)

PII Information that can be used to distinguish or trace an individual 's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
(*ODNI Intelligence Community Policy Framework for CAI*, May 2024)

sensitive activities Activities that over an extended period of time establish a pattern of life; reveal personal affiliations, preferences, or identifiers; facilitate prediction of future acts; enable targeting activities; reveal the exercise of individual rights and freedoms (including the rights to freedom of speech and of the press, to free exercise of religion, to peaceable assembly—including membership or participation in organizations or associations—and to petition the government); or reveal any other activity the disclosure of which could cause substantial harm, embarrassment, inconvenience, or unfairness to the U.S. person or person in the United States who engaged in the activity.
(*ODNI Intelligence Community Policy Framework for CAI*, May 2024)

Sensitive CAI

CAI is considered sensitive if the CAI is purchased from a commercial entity through a commercial transaction for a fee or made available by the commercial entity at no cost through a commercial transaction that normally would involve a fee (e.g., a free trial offering of CAI); and the CAI is known or reasonably expected to contain:

a. a substantial volume of personally identifiable information (PII) regarding U.S. persons; or

b. a greater than de minimis volume of:

i. sensitive data, which is defined as data that captures personal attributes, conditions, or identifiers that are traceable to one or more specific U.S. persons, either through the dataset itself or by correlating the dataset with other available information; and that concerns the U.S. person's or U.S. persons' race or ethnicity, political opinions, religious beliefs, sexual orientation, gender identity, medical or genetic information, financial data, or any other data the disclosure of which would have a similar potential to cause substantial harm, embarrassment, inconvenience, or unfairness to the U.S. person or U.S. persons described by the data; or

ii. data that captures the sensitive activities of U.S. persons or persons in the United States, with sensitive activities defined as activities that over an extended period of time establish a pattern of life; reveal personal affiliations, preferences, or identifiers; facilitate prediction of future acts; enable targeting activities; reveal the exercise of individual rights and freedoms (including the rights to freedom of speech and of the press, to free exercise of religion, to peaceable assembly—including membership or participation in organizations or associations—and to petition the government); or reveal any other activity the disclosure of which could cause substantial harm, embarrassment, inconvenience, or unfairness to the U.S. person or person in the United States who engaged in the activity.

Notwithstanding the above criteria, Sensitive CAI does not include:

- newspapers or other periodicals; weather reports; books, journal articles, or other published works; public filings or records; or similar documents or databases, whether accessed through a subscription or accessible free of cost; or

- limited data samples made available so an IC element can evaluate whether to purchase the full dataset and not accessed, retained, or used for any other purpose unless assessed in accordance with Section II.B of this Policy Framework.

(*ODNI Intelligence Community Policy Framework for CAI*, May 2024)

Sensitive Data — Data that captures personal attributes, conditions, or identifiers that are traceable to one or more specific U.S. persons, either through the dataset itself or by correlating the dataset with other available information; and that concerns the U.S. person's or U.S. persons' race or ethnicity, political opinions, religious beliefs, sexual orientation, gender identity, medical or genetic information, financial data, or any other data the disclosure of which would have a similar potential to cause substantial harm, embarrassment, inconvenience, or unfairness to the U.S. person or U.S. persons described by the data.
(*ODNI Intelligence Community Policy Framework for CAI*, May 2024)

USPI — Information that is reasonably likely to identify one or more specific U.S. persons. USPI may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons. Determining whether information is reasonably likely to identify one or more specific U.S. persons in a particular context may require a case-by-case assessment by a trained intelligence professional. USPI is not limited to any single category of information or technology. Depending on the context, examples of USPI may include: names or unique titles; government-associated personal or corporate identification numbers; unique biometric records; financial information; and street address, telephone number, and Internet Protocol address information. USPI does not include:
• A reference to a product by brand or manufacturer's name or the use of a name in a descriptive sense, as, for example, Ford Mustang or Boeing 737; or
• Imagery from overhead reconnaissance or information about conveyances (e.g., vehicles, aircraft, or vessels) without linkage to additional identifying information that ties the information to a specific U.S. person.
(DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 8 Aug 2016)

Annex D

References

(a) *Intelligence Community Policy Framework for Commercially Available Information*, May 2024 (U)

(b) DoD Manual (DoDM) 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 8 Aug 2016 (U)

(c) DoD Directive (DoDD) 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)*, 20 Aug 2020 (U)

(d) DoD Instruction (DoDI) 3115.12, *Open Source Intelligence (OSINT)*, 16 Jul 2020 (U)

(e) AFI 14-104, *Oversight of Intelligence Activities*, 16 Apr 2007 (U)

(f) AFI 14-404, *Intelligence Oversight*, 3 Sep 2019 (U)

(g) AFMAN 14-405, *Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR)*, 11 May 2020 (U)

(h) DAFMAN 16-201, *Department of the Air Force Foreign Disclosure and Technology Transfer Program*, 19 Jan 2021 (U)

(i) AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*, 4 Aug 2016 (U)

(j) Intelligence Community Directive (ICD) 203, *Analytic Standards*, 21 Dec 2022

(k) ICD 206, *Sourcing Requirements for Disseminated Analytic Products*, 22 Jan 2015

(l) ICD 208, *Maximizing the Utility of Analytic Products*, 9 Jan 2017 (U)

(m) ICD 503, *Intelligence Community Information Technology Systems Security Risk Management*, 21 Jul 2015 (U)

(n) ICD 710, *Classification Management and Control Markings System*, 21 Jun 2013 (U)

(o) Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, 28 Jul 2016 (U)

(p) NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Apr 2010 (U)

(q) Air Force Records Disposition Schedule as of 1 Nov 2021