U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

National Policy

DRAFT ORDER 1200.22F

Effective date:
09/30/2025

SUBJ: External Release of National Airspace System (NAS) Data

This order prescribes Federal Aviation Administration policies and procedures for managing the release of National Airspace System (NAS) data to entities outside of the FAA through its NAS Data Release Board (NDRB). Many of the information systems managed by the Air Traffic Organization, from which these external releases are sourced, contain sensitive and nonpublic NAS data. The unauthorized release of sensitive NAS data adversely impacts the Nation's security interests, including the Operations Security of sensitive government missions and the security of the NAS itself. This order ensures external releases are authorized and appropriately protect sensitive and nonpublic NAS data. This order also aligns the NDRB process with provisions of the Open, Public, Electronic, and Necessary Government Data Act facilitating the broad sharing of non-sensitive public NAS data.

Bryan Bedford
Administrator

TABLE OF CONTENTS

Chapter 1. General Information 1-1
1. Purpose of this Order. 1-1
2. Audience. 1-2
3. Where to Find this Order. 1-2
4. What this Order Cancels 1-2
5. Explanation of Changes. 1-2
6. Distribution. 1-3

Chapter 2. Application 2-1
1. Authority. 2-1
2. Policy. 2-2
3. Exceptions. 2-4
4. Scope of NDRB Evaluation. 2-6
5. FAA Responsibilities. 2-8

Chapter 3. NAS Data Release Board Evaluation Process 3-1
1. NDRB Evaluation Process Overview 3-1
2. When and What Type of NDRB Evaluation is Required. 3-4
3. Full and Targeted NDRB Evaluations Differentiated. 3-5
4. Prioritization of NDRB Evaluations 3-6
5. Timelines for Contacting the NDRB Secretariat. 3-6
6. NDRB Evaluator and Participant Responsibilities 3-7
7. Integration with the AMS Lifecycle. 3-9
8. NDRB Coordination with ATO CRB, TIS ARB, and NAS CCB.. 3-10
9. Procedures For ATO System Disconnects and NAS Data Subscription Terminations.. 3-11

Appendices

Appendix A. Acronyms A-1
Appendix B. Types of NAS Data and Related Definitions B-1
Appendix C. Related Directives, Publications, and Documents C-1
Appendix D. NDRB Forms and Applications D-1
Appendix E. Sustained External Release E-1
Appendix F. Focused External Release F-1

Appendix G. Sensitive External Release G-1
Appendix H. Information Security Requirements H-1
Appendix I. NDRB Evaluation Process Documentation Requirements I-1

Chapter 1. General Information

1. PURPOSE OF THIS ORDER.

a. This order establishes Federal Aviation Administration (FAA) policies and processes to manage the release of National Airspace System (NAS) data to entities outside of the FAA through its NAS Data Release Board (NDRB). Many of the information systems managed by the Air Traffic Organization (ATO), from which these external releases are sourced, contain sensitive and nonpublic NAS data, including Sensitive Unclassified Information (SUI) and Controlled Unclassified Information (CUI). Access to sensitive NAS data by unauthorized persons could adversely impact U.S. security interests, including the Operations Security (OPSEC) of sensitive government missions and the security of the NAS itself. This order ensures external releases are approved and appropriately protect sensitive and nonpublic NAS data in a manner that ensures compliance with the Federal Information Security Modernization Act of 2014 (FISMA).

b. The NDRB process prescribed by this order addresses multiple types of sensitive NAS data: Sensitive Flight Data (SFD), NAS Sensitive Technical Information (NAS STI), and ATO Cybersecurity Authorization and Vulnerability Information (ATO CAVI) but is primarily focused on protecting SFD and NAS STI due to the heightened risks associated with OPSEC and critical infrastructure, respectively. SFD encompasses all flight data related to any individual flight associated with a sensitive government mission conducted for the purposes of national defense, homeland security, intelligence, or law enforcement. This includes flights conducted by Federal Departments or Agencies (D/As) as well as State, Local, Territorial, and Tribal (SLTT) law enforcement agencies. Unauthorized disclosure of SFD could compromise the OPSEC of these operations, adversely affecting mission objectives and impacting the safety of persons or property in the air or on the ground. The NDRB process supports the OPSEC requirements of National Security Decision Directive (NSDD) 298, *National Operations Security Program*, and the security risk management requirements of National Security Memorandum (NSM)-22, *National Security Memorandum on Critical Infrastructure Security and Resilience*, by prohibiting the unauthorized disclosure of SFD and NAS STI, and conditioning authorized external releases of SFD and NAS STI on the satisfaction of need-to-know, duty-to-protect, and data protection requirements.

c. This order also facilitates broad external sharing by the FAA of non-sensitive NAS data with the public in compliance with the Open, Public, Electronic and Necessary Government Data Act of 2018 (*OPEN Government Data Act*). The prescribed NDRB process includes Chief Data Officer (CDO) participation to facilitate identifying non-sensitive NAS data, which qualify as Public Data Assets and Open Government Data Assets.

NOTE-
See Appendix B for definitions of the types of NAS data.

REFERENCE-
NSDD 298, National Operations Security Program*; and* OPEN Government Data Act.

2. AUDIENCE.

This order applies to all ATO offices and facilities involved in any aspect of the external release of NAS data, specifically including, but not limited to: the Headquarters offices of Air Traffic Services (AJT), Technical Operations Services (AJW), Program Management Organization (PMO/AJM), System Operations Services (AJR), and Mission Support Services (AJV); the three Service Centers (SC), including their subordinate groups responsible for noise abatement issues; and Air Traffic Control (ATC) field facilities, which may receive direct requests from entities outside of the FAA for access to NAS data. This order also applies to Lines of Business (LOB) and Staff Offices (SO) outside of the ATO, which may become involved with the external release of NAS data, including, but not limited to: the Office of NextGen (ANG); Information & Technology Services (AIT), including the Office of the Chief Data Office (CDO/ADO) and the Information Security & Privacy Service (AIS); the Office of the Chief Counsel (AGC); Security and Hazardous Materials Safety (ASH). This order also applies to the interaction between the FAA, principally through the NDRB, with Federal D/As with OPSEC and other equities related to sensitive NAS data.

3. WHERE TO FIND THIS ORDER.

This order can be found on the MyFAA employee website at https://employees.faa.gov/tools_resources/orders_notices/ and is available to the public at http://www.faa.gov/regulations_policies/orders_notices.

4. WHAT THIS ORDER CANCELS.

This order cancels Order 1200.22E, *External Requests for NAS Data*, dated January 1, 2012, and FAA Notice 1200.21, *Continuation of Multiple Pen and Ink Changes to FAA Order 1200.22E*.

5. EXPLANATION OF CHANGES.

This order significantly updates the previous FAA policies and procedures managing the external release of NAS data through the NDRB. The changes incorporated into this order clarify and modernize how the NDRB process protects sensitive NAS data by providing procedures tailored to three defined categories of external release: *Sustained External Release*, *Focused External Release*, and *Sensitive External Release*; and reinforcing the security boundary of the NAS. It modernizes the NDRB process to better align with the information security requirements of Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, the Federal Information Security Modernization Act of 2014 (FISMA), Department of Transportation (DOT) Order 1351.37, *Departmental Cybersecurity Policy* and the accompanying *DOT Cybersecurity Compendium*, DOT Order 1650.5, *Controlled Unclassified Information Program*, FAA Order 1370.121, *FAA Information Security and Privacy: Policy* and its supplemental implementing directives, FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI)*, FAA Order 1375.1F, *Data and Information Management Policy*, and FAA Order 1800.66A, *Configuration Management Policy*. This revised order also expands participation in the NDRB to facilitate FAA compliance with the *OPEN Government Data Act*. The changes made by this order prominently include:

a. Chapter 1 (General Information). This chapter provides new, detailed administrative information such as purpose, audience, explanation of changes, and background.

b. Chapter 2 (Application). This chapter provides new information substantially expanding the description of relevant FAA policy and authority, the scope of the NDRB, and FAA responsibilities.

c. Chapter 3 (NAS Data Release Board Evaluation Process). This chapter provides new information substantially expanding the description of full and targeted NDRB evaluations; the priority of NDRB evaluations; when and how to contact the NDRB; an overview of the NDRB process and participant functions; and the linkage between the NDRB and other ATO system and data management related boards.

d. Appendix A (Acronyms). This appendix provides a new list of acronyms pertinent to this order.

e. Appendix B (Types of NAS Data and Related Definitions). This appendix provides a significantly expanded list of definitions for terms of art used in this order, including different types of NAS data.

f. Appendix C (Related Directives, Publications, and Documents). This appendix provides a new, significantly expanded list of reference documents pertinent to this order.

g. Appendix D (NDRB Forms and Applications). This appendix includes the FAA Form 1200-5, *NAS Data Release Request*, and instructions for form completion. Minor format changes were made to the form.

h. Appendices E (Sustained External Release), F (Focused External Release), and G (Sensitive External Release). These appendices provide new procedures for NDRB evaluation tailored to each of the three categories of external release: sustained, focused, and sensitive NAS data containing SUI/CUI.

i. Appendix H (Data Protection). This appendix provides new information on the data protection requirements that must be met by External Recipients authorized by the NDRB to access unfiltered NAS surveillance containing SFD and other sensitive non-public NAS data.

j. Appendix I (NDRB Evaluation Process Documentation Requirements). This appendix provides new, substantially more detailed information on the documentation and other supporting material required to aid a NAS data release request evaluation and outlines the NDRB Decision Record minimum authorizations and conditions to be annotated.

6. DISTRIBUTION.

This order is available online and will be distributed electronically to all offices that subscribe to receive email notification and/or access to it through the FAA website (http://www.faa.gov/regulations_policies/orders_notices/).

Chapter 2. Application

1. AUTHORITY.

a. The FAA authority to release non-sensitive NAS data is pursuant to title 49, United States Code (49 U.S.C), section 106, subsections (1) and (m) or other appropriate authority.

b. The FAA authority to release sensitive NAS data containing SUI/CUI to an external non-federal entity in accordance with prescribed cybersecurity system and information protections is pursuant to FISMA, specifically title 44, U.S.C. (44 U.S.C.), section 3554, subsection (a)(3)(A) or other appropriate authority.

c. The FAA authority to protect SUI/CUI contained in NAS data from unauthorized disclosure depends on the specific type of SUI/CUI. There are primarily three ATO information types that can be present in sensitive NAS data that must be protected as SUI/CUI: SFD, NAS STI, and ATO CAVI. SFD may include multiple categories of SUI/CUI, as described in subparagraphs b(1) through b(3) below. NAS STI and ATO CAVI must be protected as Sensitive Security Information (SSI). SFD, NAS STI, and ATO CAVI are defined in Appendix B.

NOTES-

1. Proprietary information may also be contained in NAS data. Although proprietary information is not a specific ATO information type, it may be exempt from public release under Freedom of Information Act (FOIA), Exemption 4. Proprietary NAS data is defined in Appendix B. Consultation with Security and Hazardous Materials Safety (ASH), Office of Infrastructure Protection, Information Safeguards Division (AXF-200) is suggested when proprietary NAS data is present in an FAA system. AXF-200 may determine that the data is not suitable for external release and should be protected as For Official Use Only in accordance with FAA Order 1600.75. In addition to proprietary information being potentially exempt from release under FOIA, it may be SUI/CUI that needs to be protected. Designation of information as SUI/CUI does not automatically confer exemption from release under FOIA.

2. Personally Identifiable Information (PII) may also be contained in NAS data and is subject to the restrictions in 5 U.S.C. § 552a, the Privacy Act of 1974. Consultation with the FAA Chief Privacy Office is suggested when PII is present in data requested for external release.

(1) SFD pertaining to sensitive Department of Defense (DoD) operations has been designated by that Department as Department of Defense Critical Infrastructure Security Information (DCRIT) and is to be protected in accordance with Title 10 United States Code Section 130e (10 U.S.C. § 130e), *Treatment under Freedom of Information Act of certain critical infrastructure security information*.

(2) SFD pertaining to sensitive Department of Homeland Security (DHS) operations has been designated by that Department as SSI and is to be protected accordingly pursuant to Title 49 Code of Federal Regulations Section 1520.5 (49 CFR § 1520.5), *Sensitive security information*.

(3) SFD pertaining to sensitive Department of Justice (DOJ) operations has been designated by that Department as For Official Use Only (FOUO) and is to be protected

accordingly, including the application of FOIA withholdings pursuant to 5 U.S.C. § 552 (b)(7)(E, F).

NOTES-
1. Both DCRIT and SSI are categories of CUI, a U.S. Government-wide program for managing unclassified information that requires safeguarding or dissemination controls established by Executive Order (EO) 13556, Controlled Unclassified Information*, and is governed by 32 CFR Part 2002,* Controlled Unclassified *Information. USDOT Order 1650.5, Controlled Unclassified Information Program, implements the above directives. However, at the time of the publication of this order, the FAA had not yet fully implemented a CUI program. Once FAA implements CUI, the FOUO information will be protected in accordance with applicable CUI categories.*

2. This Order focuses on data protection requirements mandated by FAA Order 1600.75, Protecting *Sensitive Unclassified Information (SUI), but is also informed by CUI-related requirements regarding the protection of SFD's DCRIT and SSI elements in accordance with FAA Order 1370.121, FAA Information Security and Privacy: Policy. Once the FAA fully implements a CUI program, For Official Use Only (FOUO) will no longer be recognized as a protected information category, and information will be protected in accordance with applicable CUI categories.*

d. The NDRB process protects NAS data from unauthorized release to external entities and operates under the authority of the FAA Administrator.

e. The FAA Administrator:

(1) Delegates to the Chief Operating Officer, COO / AJO-0, who heads the ATO, the authority to establish policies and procedures for and provide management oversight of the NDRB and the NAS data release process.

(2) Directs FAA Lines of Business and Staff Offices (LOB/SO) to support the NDRB evaluation process, in accordance with this order.

f. The ATO COO is the information owner of NAS data, wherever it resides.

REFERENCE-
FAA Order 1370.121, FAA Information Security and Privacy: Policy, Governance Supplemental Implementing Directive*, section 2.6.*

g. The ATO Authorizing Official (AO) is the authority responsible for evaluating the risk to the NAS and authorizing the connection for and release of any sensitive NAS data when that release is subject to NDRB review per the policy contained in this order.

h. The Director, System Operations Security, AJR-2, subject to the direction of AJO-0 and the Vice President for System Operations Services, AJR-0, serves as Chair of the NDRB, coordinates the activities of the NDRB, and manages the NDRB Secretariat.

REFERENCE-
FAA Order 1370.121, FAA Information Security and Privacy: Policy, Governance Supplemental Implementing Directive*, section 2.6.1.*

2. POLICY. It is FAA policy to:

a. Release NAS data to external entities through secure enterprise connections (i.e., external connections that are established through FAA-approved domain boundary protection

gateways) only as authorized by the ATO AO, and approved by the Director, System Operations Security, following the prescribed NDRB processes.

NOTES-
1. *For purposes of this order, the term "external" means either a non-FAA connection or an entity outside the FAA.*

2. *An approved domain boundary protection gateway is a mechanism that securely enables a connection to the FAA network infrastructure from an external source. All domain boundary protection gateways are documented in a system security authorization approved by the ATO Authorizing Official (AO) and the FAA Chief Information Officer (CIO).*

REFERENCE-
FAA Order 1370.121, FAA Information Security and Privacy: NIST Controls Supplemental Implementing Directive, Access Control (AC)-4(2).

b. Ensure all existing FAA legacy non-secure external connections (i.e., external connections that are not using an FAA-approved domain boundary protection gateway) are immediately reported to the ATO AO via the ATO Cybersecurity Review Board (CRB) Chair, to expeditiously replace or terminate the connection as appropriate.

c. Approve only those external connections that are authorized by the ATO AO or Chief Information Security Officer (CISO), such as the NAS Enterprise Security Gateway (NESG) or other approved domain boundary protection gateway. Only approve an external direct connection, defined as an external connection adapted into the NAS Domain via a NAS Change Proposal (NCP), to access NAS data for the purpose of safety-critical Air Traffic Control (ATC) separation services (e.g., ATC services performed by qualified DoD personnel), after that direct connection has been approved by the NAS Configuration Control Board (CCB) and authorized by the ATO AO.

NOTE-
Direct connections to NAS surveillance systems, such as NAS radar, and automation platforms, such as Standard Terminal Automation Replacement System (STARS), are managed through the NAS CCB via adjudication of an NCP request.

d. Require external releases of sensitive NAS data (i.e., NAS data containing SFD or other SUI/CUI) to satisfy the need-to-know, legally binding duty-to-protect, and data protection requirements prescribed by this order.

e. Ensure that any external non-Federal entity requesting access to sensitive NAS data meets the prerequisite requirements in this order, including implementation of all data protection requirements per appendices G and H of this order.

f. Support the release of public, non-sensitive NAS data through processes outlined in Appendices E, F, G, and H to the extent required by the OPEN Government Data Act. Non-sensitive NAS data is defined as NAS data that does not, in its original form, contain SUI/CUI or from which all SUI/CUI has been removed by filtering and/or redaction, removal, or otherwise withholding.

g. Suspend or terminate external releases as directed by the ATO AO when necessary to ensure the protection of SUI/CUI, for national security or cybersecurity reasons, or to support higher priority FAA mission needs. Also provide notification to affected External Recipients as time permits.

h. Ensure all external requests to access NAS data from FAA field facilities (see definition of FAA field facilities in Appendix B) are submitted to the NDRB Secretariat for coordination and adjudication by the ATO AO prior to proposed activation. Specifically, FAA field facilities must immediately consult with the NDRB Secretariat on any request for direct connections between an FAA information system and an external information system, and proposed connections from any FAA information system and/or automation platform located at an FAA field facility to external recording devices or other external equipment placed inside that FAA facility.

NOTES-
1. *FAA field facilities must route these NAS data release requests through appropriate Service Center Points of Contact (POC) to the NDRB Secretariat.*

2. *See policy statement in para. 2c. All external connections to FAA information systems and/or automation platforms and/or FAA equipment located at an FAA field facility must be established via an FAA-approved domain boundary protection gateway (e.g., the external side of the NESG).*

3. *External Information System is defined in Appendix B.*

i. Ensure all external requests to access NAS data contained in FAA online storage repositories (e.g., the Enterprise Information Management Platform and NAS Data Warehouse) are submitted to the System Owner and/or the information steward for the system of origin for the specific NAS data and adjudicated in accordance with that system of origin's NDRB Decision Record. Any connection intended to disseminate NAS data from an FAA online storage repository to an External Recipient must first be authorized by the ATO AO and then identified as an authorized connection on the NDRB Decision Record prior to operational use.

j. Approve only the use of non-sensitive NAS data for the initial testing of secure external connections with non-FAA entities (e.g., testing at the FAA Telecommunications Infrastructure (FTI) National Test Bed (FNTB) located at the William J. Hughes Technical Center for Advanced Aerospace [WJHTCAA] or other external testing activities with non-FAA entities).

NOTE-
FAA personnel must not release any FAA data to external entities, in any format, that potentially contains SFD, without first consulting with the NDRB Secretariat for analysis.

REFERENCE-
FAA Information Security & Privacy: FAA Implementation of NIST Controls Supplemental Implementing Directive, April 25, 2022, Control SA 3(2), Use of Live or Operational Data.

3. EXCEPTIONS. The policies and procedures prescribed by this order are generally not applicable for external releases of NAS data falling under one or more of the following exceptions to the NDRB process; mandatory consultation with the NDRB Secretariat must be accomplished as detailed in the specific exceptions below:

a. Federal D/A Exception. The Executive Manager of NAS Defense Programs (NDP),

AJW-B7, or designee has the authority to release NAS data, including SFD and other types of SUI/CUI, with the exception of ATO CAVI, to other Federal D/As on behalf of the Director, NAS Security and Enterprise Operations (NASEO), AJW-B. NDRB evaluation is not required for NAS data releases under this exception, although NDP may consult with the NDRB Secretariat and other NDRB evaluators as needed. NDP must secure AJR-2 approval prior to the release of any NAS data to Federal D/As from FAA information systems sponsored by AJR-2. NDP assumes the responsibility for ensuring the requisite protection of all SUI/CUI released to Federal D/As under this exception.

b. State, Local, Territorial, and Tribal Law Enforcement (SLTTLE) Exception. The Executive Manager of NDP/AJW-B7 or designee has the authority to release NAS data, including SUI/CUI, from FAA information systems for which program management is carried out by NDP to SLTTLE agencies on behalf of the Director of NASEO, AJW-B. All such releases must be done via an FAA-approved domain boundary protection gateway (e.g., the external side of the NESG) and not via any direct connection to the NAS infrastructure. NDP must secure AJR-2 approval prior to the release of any NAS data to SLTTLE from FAA information systems sponsored by AJR-2. SLTTLE agency requests for NAS data contained in FAA information systems not managed by NDP must go through NDRB evaluation. NDP assumes the responsibility for ensuring the requisite protection of all SUI/CUI released to SLTTLE agencies under this exception and must notify the NDRB Secretariat to initiate coordination with impacted I/A partner(s), as appropriate.

c. ATO Cybersecurity Authorization and Vulnerability Information (ATO CAVI) Exception. The ATO Authorizing Official and/or designee has the authority to release ATO CAVI data to other Federal D/As. NDRB review is not required for the external release of ATO CAVI under this exception. The NDRB Secretariat must direct any external request for ATO CAVI data to the ATO CRB Chair for action. The ATO AO and/or designee also has the authority to release ATO CAVI data to other external entities on a case-by-case basis once need-to-know has been validated by the ATO AO and/or designee and confirmed by AXF-200. The ATO AO and/or designee assumes responsibility for ensuring the requisite protection of all ATO CAVI released to another Federal D/A or other external entity under this exception.

d. FAA Contract or Grant Exception. NAS data that is specified as Government Furnished Information (GFI) in an FAA contract or grant agreement with an external entity, and which is necessary for the performance of that FAA contract or grant agreement, may be released externally on the authority of the Contracting Officer (CO) without NDRB evaluation. The responsible CO and FAA LOB/SO contract/grant sponsors must coordinate with the NDRB Secretariat to receive a determination on whether their NAS data set contains any SUI/CUI prior to contract or grant agreement release. If the NAS data that is specified as GFI does contain SUI/CUI, the NDRB must be used as a resource to facilitate assistance with contractual data protection language and/or requisite data protection measures. The NDRB Secretariat must advise the Chair of the ATO CRB and receive a determination of any impact on the affected system's "Authority to Operate." All such connections must be made via an FAA-approved domain boundary protection gateway (e.g., the external side of the NESG) and authorized by the appropriate AO or CISO.

NOTE -
Contract support for FAA programs, information systems, second-level engineering, operations support, and information security is considered to be internal NAS data sharing.

e. FOIA Exception. The external release of NAS data in response to FOIA requests involving NAS data does not require NDRB evaluation. However, if the responsive records to a FOIA request may contain SUI/CUI, the ATO Headquarters FOIA Team or ATO Service Center Management and Support Team (MAST) must contact the NDRB Secretariat for guidance from the ATO Cybersecurity Group (ACG/AJW-B4) to confirm the existence of SUI/CUI. If there is SUI/CUI present, the ATO Headquarters FOIA Team or Service Center MAST will determine if there is an applicable FOIA exemption for the purposes of withholding the record, or portions thereof. To avoid confusion, the appropriate FOIA office must contact the NDRB Secretariat for guidance in situations where the presence of SUI/CUI in the NAS data contained in the responsive records is unknown. In addition, appropriate coordination with internal FAA LOB/SOs and Federal D/A aviation stakeholders must be effected prior to the sharing of sensitive NAS data.

f. International Agreement Exception. International agreements between the FAA, other Federal D/As, and foreign entities do not require NDRB evaluation. However, many international agreements involve the sharing of NAS surveillance and/or air traffic automation data that contains one or more types of SUI/CUI. The FAA Office of International Affairs (API) and the ATO International Office (AJV-I) must consult with the NDRB Secretariat, ACG and the Office of the Chief Counsel, International Affairs and National Security Law Division, International Law Team (AGC-710) and the Information, Data and Technology Division (AGC-400), to ensure adequate protection language for any SUI/CUI contained in the relevant NAS data set(s) is included in the agreement documentation. In addition, appropriate coordination with internal FAA LOB/SOs, Federal D/A aviation stakeholders, and appropriate Department of State (DOS) office (recognizing the need to protect ongoing bilateral negotiations) must be effected for FAA international agreements that involve the sharing of sensitive NAS data. All such connections must be authorized by the ATO AO and made via an FAA-approved domain boundary protection gateway (e.g., the external side of the NESG).

g. Aircraft Certification Exception. (RESERVED – *Situations in which FAA personnel obtain post-flight aircraft navigational information for specific operators or manufacturers related to aircraft certification testing will be detailed in subsequent updates to this order*.)

h. National Transportation Safety Board (NTSB) Exception. FAA release of NAS data to the NTSB, which the agency is obligated by applicable law, regulation, or policy to provide in furtherance of that Board's statutory functions, does not require NDRB evaluation. However, provision of NAS surveillance and/or air traffic automation data is likely to contain one or more types of SUI/CUI. FAA LOB/SOs engaged in the provision of NAS data to the NTSB must consult with the NDRB Secretariat to ensure adequate protection for any SUI/CUI contained in the NAS data set is in place.

4. SCOPE OF NDRB EVALUATION.

d. NDRB evaluation is required prior to external releases of all NAS data, inclusive of both sensitive and non-sensitive NAS data, unless the proposed release is covered by an exception

cited in paragraph 3 of this chapter.

e. FAA information systems with an existing NDRB Decision Record must also undergo NDRB evaluation for a subsequent system release or version when one or more NDRB triggers apply per the procedures in Appendices E, F, and G.

f. NDRB evaluation is required regardless of where and in what medium the NAS data involved is stored, the FAA information system or environment in which it is located, the technological means that the FAA will use to share the data with External Recipients, and whether the data is real-time, near real-time, or historical.

g. The scope of the NDRB evaluation for FAA information systems containing SUI/CUI is a system-wide approach. It is not limited to an evaluation of only the changes to that information system because the evaluation must assess the ability of the whole system to protect SUI/CUI during transmission to external data recipients. During NDRB evaluation, the evaluators examine the following items (as applicable): external data recipient(s) and the intended use of the data, legally binding agreements or data access agreements, external data connections, external information system(s) and architecture, the validated status of the required security controls as applied to the external system to meet SUI/CUI protection requirements, and the status of the System Owner's SUI/CUI protection mitigation plan.

NOTE-
Although the NDRB evaluation is separate and distinct from the evaluations conducted by the ATO CRB and the Telecommunications Integrated Services (TIS), Architecture Review Board (ARB), the NDRB Decision Record may inform the decision processes of those boards. Likewise, the decisions of those boards may inform the NDRB evaluation.

h. Unless the proposed NAS data release is covered by an exception cited in paragraph 3 of this chapter, NDRB evaluation is required for external release of all sensitive and non-sensitive NAS data, including:

(1) NAS data shared externally via connections to the NAS infrastructure and FAA secure external connection gateways in both testing and operational configurations.

(2) Real-time, near real-time, and historical NAS data.

(3) Any NAS data shared externally via connections outside of the NAS infrastructure, such as but not limited to: Cloud computing technology and/or external connections to FAA online storage repositories, Application Programming Interfaces (API), the Mission Critical Operating Environment (OE), Mission Essential OE, Administrative OE and the Research and Development (R&D) OE.

NOTE-
All external connections outside of the NAS infrastructure must be secured through FAA-approved domain boundary protection gateways.

i. NAS data sharing between FAA information system OEs, such as those mentioned above in paragraph 4e3, is considered internal NAS data sharing and not subject to the NDRB evaluations prescribed by this order.

NOTE-
Although the NDRB has no jurisdiction over internal data sharing, some of its evaluators are responsible for determining whether or not a system contains certain types of SUI/CUI. For instance, AJR-2 is the authority for determining the presence of SFD in any FAA system regardless of whether it is an external release system or not. Similarly, the ATO Cybersecurity Group (ACG/AJW-B4) is the authority for determining the presence of NAS STI in any FAA system

j. NDRB evaluation for an external request for NAS data containing SFD, or any other SUI/CUI, must not be initiated unless the prospective External Recipient meets all the prerequisite conditions detailed in Appendix H. This requirement is applicable to all requests for SFD and other SUI/CUI using the procedures in Appendix G

5. FAA RESPONSIBILITIES.

a. The COO must:

(1) Provide executive-level oversight of the NDRB's execution of FAA policies and objectives related to NAS data release.

(2) Ensure the NDRB receives the necessary support prescribed in this order from other ATO evaluation boards managed by AJM and AJW, including, but not limited to, the TIS ARB, ATO CRB, and NAS CCB.

(3) Ensure the NDRB receives the necessary support prescribed in this order from the responsible ATO Service Units.

b. The Vice President for System Operations Services (AJR-0) must:

(1) Provide executive-level oversight of the NDRB's execution of FAA policies and objectives related to NAS data release.

(2) Ensure the NDRB receives the necessary resource support from within System Operations Services.

c. The Director, System Operations Security, AJR-2, or designee must:

(1) Serve as Chair of the NDRB.

(2) Staff the NDRB Secretariat.

(3) Establish NDRB evaluator membership.

(4) Ensure an objective NDRB process.

(5) Act as the final FAA approval authority for release of NAS data that does not meet the criteria for an exception cited in paragraph 3 of this chapter in accordance with ATO AO authorization and risk response decisions for external release of sensitive NAS data.

d. The ATO Authorizing Official, AJW-1, must:

(1) Act as the official FAA authority to evaluate the risk to the NAS and authorize the connections for and release of any sensitive NAS data that does not meet the criteria for an exception cited in paragraph 3 of this chapter.

(2) Formally accept the risk to NAS systems, NAS data, other non-FAA organizations, and the National interest posed by the proposed release of sensitive NAS data to a specific external non-Federal entity, including mitigation of residual risk to an acceptable level.

e. The NDRB Secretariat must:

(1) Serve as the primary POC for the NDRB to receive, coordinate, and respond to all correspondence and questions regarding NAS data release matters under the purview of this policy.

(2) Administer the NDRB evaluation process in accordance with the policy and procedures contained in this order.

(3) Refer matters outside the scope of the NDRB to the appropriate FAA POCs.

(4) Maintain an appropriately secure official archive of NDRB documentation, including requests, NDRB Decision Records, and Administrative Records.

(5) Maintain an objective NDRB process by not serving as an External Release Sponsor or advocate for prospective External Recipients requesting access to NAS data.

(6) Ensure prospective External Recipients requesting access to NAS data containing SFD or any other SUI/CUI meet all ACG-provided data protection requirements detailed in Appendix H.

(7) Ensure ATO AO authorization of connections and acceptance of risk has been obtained for all proposed external releases of sensitive NAS data prior to coordinating final approval by the NDRB Chair on the NDRB Decision Record.

f. NDRB Evaluators must be Federal employees formally identified by their LOB/SO management to represent their LOB/SO on the NDRB.

g. FAA LOB/SOs must support the NDRB, as outlined in Chapter 3 and Appendices E, F, G, H, and I of this order; and respond to NDRB Secretariat requests in accordance with requirements in Chapter 3, Section 5 of this order.

h. In accordance with Chapter 3 of this order, AJR, AJW, PMO/AJM, ASH, AGC, and CDO/ADO offices must ensure the specified NDRB Evaluators and NDRB Subject Matter Expert (SME) participants are designated and effectively support NDRB evaluations.

i. FAA System Owners must:

(1) Comply with applicable NDRB Decision Record(s) and conditions.

(2) Submit requests for NAS data release adjudication to the NDRB Secretariat as soon as practicable, in accordance with the minimum timelines required for coordination outlined in Chapter 3, Section 5 of this order.

j. FAA External Release Sponsors must:

(1) Establish contact with NDRB Secretariat and complete all necessary coordination, collaboration, and administrative requirements to support the NDRB evaluation process as directed by this order and the NDRB Secretariat, as applicable.

(2) Maintain coordination with NDRB Secretariat throughout the NDRB process.

(3) Provide status updates to the appropriate FAA executive leadership as the originator of and/or Office of Primary Responsibility (OPR) for individual external release requests.

(4) Ensure resources, including funding, necessary for the release are allocated, as required.

k. ATO Service Center NDRB Representative. Each ATO Service Center must designate an NDRB representative to assist the NDRB with external requests for access to NAS data and/or FAA information systems maintained within ATO field facilities. ATO Service Center NDRB representatives must:

(1) Perform preliminary coordination, collaboration, and administration requirements with the prospective External Recipient(s) and the ATO field facility(ies) to complete FAA Form 1200-5. Once complete, forward the request to the NDRB Secretariat at 9-AJR-NDRB-Executive-Secretariat@faa.gov.

(2) Assist the FAA External Release Sponsor and the prospective External Recipient as needed throughout the NDRB evaluation process.

l. FAA field facilities.

(1) FAA field facilities (ATO and non-ATO) may receive external requests for a direct external connection to FAA equipment at their facility to access NAS data. FAA field facilities must not allow any external user connections unless authorized by the ATO AO and the connection is made via an FAA-approved domain boundary protection gateway, such as the NESG.

(2) All ATO field facilities must refer external requests for access to NAS data to their designated ATO Service Center NDRB representative. In the absence of an ATO Service Center NDRB representative, refer external NAS data requests directly to the NDRB Secretariat at: 9-AJR-NDRB-Executive-Secretariat@faa.gov for immediate notification to the ATO CRB Chair.

NOTE-
The ATO CRB Chair will initiate requisite coordination with the ATO AO to ensure the proposed connection for external data sharing is managed within the parameters of the system's Authority to Operate.

(3) All non-ATO facilities, including the Mike Monroney Aeronautical Center (MMAC) and the WJHTCAA, must refer external NAS data requests directly to the NDRB Secretariat at: 9-AJR-NDRB-Executive-Secretariat@faa.gov.

NOTE-
See Appendix B for the definition of FAA field facilities.

Chapter 3. NAS Data Release Board Evaluation Process

1. NDRB EVALUATION PROCESS OVERVIEW.

k. Pre-Coordination. The NDRB Secretariat must implement an NDRB evaluation pre-coordination process, which includes cooperation with the System Owner, External Release Sponsor, SFD Security Program Manager (only when SFD is involved), ACG (for all SUI/CUI), and, as needed, the External Requestor to carry out the following pre-coordination tasks before the NDRB Evaluation is started.

NOTE –
The System Owner and External Release Sponsor may be the same.

(1) Confirm if the external release requires an NDRB evaluation in accordance with paragraph 2 of this chapter and in consideration of the exceptions cited in Chapter 2, paragraph 3 of this order.

(2) Determine the category of the proposed external release if no exception applies:

(a) **Sustained External Release**. External releases of NAS data that meet the following criteria: the released NAS data is non-sensitive; the released NAS data is sourced by an FAA information system, which is designed to broadly share NAS data outside of the FAA via one or more external connections established within its security authorization boundary; and the release is intended to be sustained (i.e., has no planned end).

(b) **Focused External Release**. External releases of NAS data that meet the following criteria: the released NAS data is non-sensitive; the released NAS data is sourced by an FAA information system, which is not designed to broadly share NAS data outside and does not incorporate external connections established within its security authorization boundary; and the release is intended to be temporary, specific to an activity with a planned end.

(c) **Sensitive External Release**. External releases of NAS data that meet the following criteria: the released data is intended to contain sensitive NAS data, including SFD or other types of SUI/CUI; and the released NAS data is sourced by an FAA information system.

(3) Determine the type of NDRB evaluation needed in accordance with paragraphs 2 and 3 of this chapter.

(4) Ensure the External Release Sponsor submits an FAA Form 1200-5 to the NDRB Secretariat at 9-AJR-NDRB-Executive-Secretariat@faa.gov.

(5) Prioritize the conduct of the required NDRB evaluation in accordance with paragraph 4 of this chapter.

(6) Confirm evaluation timelines, documentation requirements, and workflow in accordance with paragraphs 4 and 5 of this chapter, and Appendix I.

l. Evaluation. Following pre-coordination, the NDRB Secretariat must implement an NDRB evaluation process in accordance with the procedures listed below.

(1) **NDRB Evaluation Package**. NDRB Secretariat must direct the development of an NDRB evaluation package with contributions from the System Owner and/or External Release Sponsor. This package will include documentation listed in Appendix I and, in the case of Sensitive External Release cases, those cited in Appendix H. NDRB evaluation packages will also include information from the NDRB Secretariat: designating an NDRB evaluation case number; guidance on evaluation timelines, including deadlines for NDRB Evaluator input; and instructions on the deliverables required of each NDRB Evaluator.

(2) **Formal Tasking**. The NDRB Secretariat will identify NDRB Evaluators, NDRB Ad Hoc Interagency Evaluators, and NDRB SME Participants needed to participate in the evaluation based on the type of NDRB evaluation applied and the particulars of the external release being evaluated. The NDRB Secretariat will formally task the selected evaluators with an NDRB evaluation package.

(3) **Sensitive External Release Ad Hoc Evaluator Inclusion**. For Sensitive External Release cases implicating the security interests of other Federal D/As, the NDRB Secretariat will invite the NDRB Ad Hoc Interagency Evaluators to participate in the evaluation activities, focusing on providing input regarding OPSEC and other security risks, and possible security risk mitigations.

(4) **Sensitive External Release Coordination Requirements with ACG.** For sensitive external release requests, the NDRB Secretariat must coordinate with ACG and with the External Requestor to ensure the External Requestor has met all requirements in Appendices G and H of this order prior to initiating NDRB Review.

(5) **Evaluation Basic Parameters**. The NDRB Secretariat will direct evaluation activities needed to, depending on the external release category and particulars of the external release being considered, address all prerequisites and evaluation factors as appropriate based on the applicable Appendices in this order. The NDRB evaluators will provide analysis, input, and recommendations for NDRB approval in the form of concurrence or non-concurrence.

(6) **Collaboration**. The NDRB Secretariat, sometimes at the request of an NDRB evaluator or the System Owner and/or External Release Sponsor, may organize collaboration activities as needed to develop a coherent evaluation of the external release being considered.

(7) **Resolution of Non-concur from ACG Evaluator(s) and/or ATO AO.** The NDRB Secretariat must ensure that any non-concur from an ACG evaluator or the ATO AO is resolved in an agreed-upon manner prior to potential NDRB approval for any proposed release of sensitive NAS data. All decisions by the NDRB for any proposed release of sensitive NAS data must be made in accordance with the risk response by the ATO AO, including stipulations on the requestor. Legal agreement(s) with the External Recipient shall be updated and signed as applicable.

(8) **Mitigations for Other Unresolved Issues**. The NDRB Secretariat must ensure that issues raised by evaluators, including non-concurrence recommendations, are each resolved in an agreed-upon manner prior to potential NDRB approval for any proposed release of sensitive NAS data. Issues may be addressed by conditions incorporated into the NDRB Decision Record or NDRB Administrative Record. The System Owner and/or External Release Sponsor must act on these conditions in addition to any stipulations as directed by the ATO AO. Legal agreement(s) with the External Recipient shall be updated and signed as applicable.

(9) **Coordination with Other Boards**. The NDRB Secretariat will, as needed, direct coordination of NDRB evaluation activities with the TIS ARB, ATO CRB, and NAS CCB.

(10) **OPEN Government Data Act Compliance**. The NDRB Secretariat will request NDRB SME participant cooperation by the Office of the (CDO/ADO) for external releases involving information systems requiring review for *OPEN Government Data Act* compliance. The CDO / ADO NDRB SME participant will cooperate with the System Owner, SFD program manager, and ACG to identify non-sensitive NAS data, which qualify as Public Data Assets and Open Government Data Assets

(11) **Adjudication Discussion**. The NDRB Secretariat will facilitate discussions among the evaluators to review and synthesize their input into a recommendation to the NDRB Chair to approve or disapprove the external release and any associated condition.

(12) **Approval or Disapproval Decision**. The NDRB Secretariat will prepare an NDRB Decision Record for Full NDRB Evaluations, which documents the approval or disapproval of the external release and any associated conditions, for signature by the NDRB Chair. For any proposed release of sensitive NAS data, the NDRB Secretariat must ensure that all NDRB decisions are made in accordance with the risk response by the ATO AO, including any required stipulations as appropriate. The NDRB must not approve a release of sensitive NAS data that is not made via an ATO AO authorized connection or not in accordance with the risk response from the ATO AO, including any associated stipulations. The NDRB Secretariat will prepare and sign an NDRB Administrative Record for Targeted NDRB Evaluations, which documents the external release's continued compliance with a pre-existing, applicable NDRB Decision Record or non-compliance with the same.

NOTE-

An external release that is not in compliance with its approved NDRB Decision Record will prompt the NDRB Secretariat to initiate a new Full NDRB Evaluation and, if necessary, recommend to the ACG CRB Chair that action be taken on system disconnects and subscription terminations as appropriate.

m. The NDRB must implement the procedures provided above, which are common to all external release categories and types of NDRB evaluation, in combination with the procedures tailored to individual external release categories, provided by Appendix F for Sustained External Release, Appendix G for Focused External Release, and Appendix H for Sensitive External Release.

n. The NDRB Secretariat will maintain an NDRB Evaluation Standard Operating Procedure (SOP) that provides detailed information for the execution of the above pre-coordination and evaluation process tasks. This SOP will be approved by the NDRB Chair.

2. WHEN AND WHAT TYPE OF NDRB EVALUATION IS REQUIRED.

a. All external releases of NAS data in an FAA system must be approved by the NDRB through its evaluation process unless the proposed release is covered by an exception cited in Chapter 2, paragraph 3 of this order. NDRB evaluations must be conducted when one or more of the following criteria are met:

(1) A System Owner of a system containing NAS data and/or an External Release Sponsor requests an NDRB evaluation, and the NDRB Secretariat agrees to proceed.

(2) A new external release is being planned. This includes the initial deployment of new FAA information systems designed to broadly share NAS data with external entities.

(3) An External Release Sponsor or External Requestor requests approval of a new external release of NAS data.

(4) The data protections incorporated into an external release previously approved by the NDRB may be affected by a revision to the originating FAA system or a change to other aspects of the release, such as the means of transporting the data.

(5) A SUI/CUI spillage incident involving the external release of NAS data is reported in a timely manner (reports will be made to the FAA Security Operations Center (SOC)).

(6) The System Owner of the system originating the data external release requests an NDRB evaluation.

(7) The external release is approved by an NDRB Decision Record issued more than three years prior.

(8) An evaluation is mandated by a relevant legal requirement, including an agreement or contract governing the external release.

(9) Use of contracted private entities for Flight Information Services (FIS), via subscription agreements, necessary for flight operations (e.g., flight planning, aircraft and pilot-dispatch interface and management, and supporting communications) involves the external release of flight data pertaining to their air operations, which may include SFD and SUI/CUI (particularly with respect to DoD contracted services).

NOTE-
These contracted private entity-type systems are not engineered to broadly share NAS data with the public (i.e., no external connection designed to broadly share data), and no SFD filtering is required. NDRB approval is required prior to initial operational deployment of these types of systems or, for systems without an existing NDRB Decision Record, at the next subsequent operational update.

b. The NDRB Secretariat will generally require Full NDRB evaluations for novel proposed external releases and external releases previously approved by the NDRB undergoing changes materially affecting established data protections and other conditions of that approval.

c. The NDRB Secretariat will generally require Targeted NDRB evaluations for external releases previously approved by the NDRB that are undergoing changes unlikely to materially affect established data protections and other conditions of that approval.

d. The NDRB Secretariat will apply the more detailed triggers for Full and Targeted NDRB evaluations prescribed for each of the three categories of external release by the supporting appendices to this order: Sustained External Release (See Appendix E); Focused External Release (see Appendix F); and Sensitive External Release (See Appendix G).

3. FULL AND TARGETED NDRB EVALUATIONS DIFFERENTIATED.

a. Full NDRB Evaluation. NDRB evaluations of this type entail a comprehensive examination of qualifying external release, including the aspects of the originating FAA information system and transport of the NAS data potentially affecting the protection of any sensitive NAS data, including SUI/CUI. Key characteristics:

(1) Typically address novel proposals for external release of NAS data that have not been evaluated by the NDRB previously (excepting those Full NDRB Evaluations triggered by criteria cited by paragraph 2 of this chapter).

(2) Necessitate the participation of all pre-designated FAA NDRB Evaluators and NDRB Ad Hoc Interagency Evaluators selected by the NDRB Secretariat.

(3) Produce an NDRB Decision Record signed by the NDRB Chair, which formally approves the external release and may include detailed conditions with which the System Owner, External Release Sponsor, and External Recipient must comply.

(4) Formally initiate with the NDRB Secretariat via email to 9-AJR-NDRB-Executive-Secretariat@faa.gov by either the System Owner or the External Release Sponsor when one or more of the applicable NDRB triggering events apply as annotated in paragraph 2 of this chapter and Appendices E, F, or G.

NOTES-

1. *The program management office or second-level engineering office typically represents the System Owner for FAA systems containing NAS data.*

2. *Major system releases with changes that do not affect data sharing with external entities in any way do not generally need NDRB evaluation unless one of the triggering events in applicable appendix applies.*

3. *Bug fixes or system patches for a current version or release do not generally need NDRB evaluation.*

b. Targeted NDRB Evaluation. NDRB evaluations of this type entail a narrow examination of qualifying external releases, which focus on changes to the originating FAA information system or other aspects of the release, such as the means of transporting the data unlikely to affect the data protection and other conditions prescribed by the pre-existing, applicable NDRB Decision Record. Key characteristics:

(1) Typically address external releases of NAS data that have been previously evaluated by the NDRB and approved by an NDRB Decision Record.

(2) Only necessitate the participation of a limited set of NDRB evaluators selected by the NDRB Secretariat, typically only including the SFD Program Manager, and the evaluators from the ACG/AJW-B4 and the Office of Infrastructure Protection (AXF).

(3) Produce an NDRB Administrative Record signed by the NDRB Secretariat, which confirms the subject external release continues to comply with the existing NDRB Decision Record and may note changes to the originating FAA system or other aspects of the release.

(4) Formally initiated with the NDRB Secretariat via email to 9-AJR-NDRB-Executive-Secretariat@faa.gov by either the System Owner or the External Release Sponsor when one or more of the applicable NDRB triggering events apply as annotated in paragraph 2 of this chapter and Appendices E, F, or G.

4. PRIORITIZATION OF NDRB EVALUATIONS.

a. The NDRB Secretariat must manage the sequencing of NDRB evaluations according to the criticality of the external release meeting the triggering criteria cited by paragraph 2 of this chapter. The order in which System Owners and External Release Sponsors request NDRB evaluations will be considered by the NDRB Secretariat but is not determinative. In addition, the NDRB Secretariat may conduct multiple NDRB evaluations in parallel. The NDRB will determine criticality based on multiple factors, including:

(1) Operational need to support the FAA's Air Navigation Services (ANS) and other NAS demands.

(2) Program schedule considerations, including critical milestones and deadlines driven by the Acquisition Management System (AMS). See paragraph 7 of this chapter.

(3) Need to contain and correct potential spillage of sensitive NAS data.

(4) Expected complexity and resource requirements for the NDRB evaluation

(5) Overall workload demands on the NDRB Secretariat and NDRB Evaluators.

5. TIMELINES FOR CONTACTING THE NDRB SECRETARIAT.

System Owners and External Release Sponsors requesting NDRB evaluations should initiate coordination by contacting the NDRB Secretariat at 9-AJR-NDRB-Executive-Secretariat@faa.gov in accordance with the guidance below. These timelines are established to mitigate the potential for adverse impacts to the cost and schedule for an external release and associated program. NDRB evaluation requests:

a. Necessitating testing with External Recipients through the FNTB: At least 4 months prior to testing.

b. For new Sustained External Releases which have not been previously approved by an existing NDRB Decision Record: At least 12 months prior to operational deployment.

c. For changes to Sustained External Releases previously approved by an existing NDRB Decision Record: At least 6 months prior to operational deployment of a revision.

d. For new Focused External Releases, which have not been previously approved by an existing NDRB Decision Record: At least 6 months prior to the desired release of NAS data.

e. For changes to Focused External Releases previously approved by an existing NDRB Decision Record: At least 6 months prior to the desired release of NAS data under the new conditions.

f. For new Sensitive External Releases, which have not been previously approved by an existing NDRB Decision Record: At least 24 months in advance of the requested date for provisioning of NAS data containing SUI/CUI.

g. For changes to Sensitive External Releases previously approved by an existing NDRB Decision Record: At least 12 months in advance of the requested date for provisioning of NAS data containing SUI/CUI.

NOTE-
FAA systems containing SUI/CUI and/or individual requests for access to NAS data containing SUI/CUI are generally the most labor-intensive and time-consuming evaluations conducted by the NDRB.

REFERENCE –
See applicable appendices for external release categories: sustained (Appendix E), focused (Appendix F), or sensitive (Appendix G).

6. NDRB EVALUATOR AND PARTICIPANT RESPONSIBILITIES.

The NDRB's conduct of efficient and effective NDRB evaluations rely on the active participation of NDRB Evaluators, NDRB Ad Hoc Interagency Evaluators, and NDRB SME Participants. The responsibilities of these participants in the NDRB evaluation process are outlined below and further detailed (e.g., exact deliverables and mandatory timelines) in the NDRB Evaluation SOP.

a. NDRB Evaluators. The NDRB Secretariat will request the participation of the NDRB Evaluators listed below in all Full NDRB Evaluations. NDRB Evaluators are required to:

(1) Confirm the absence of any sensitive NAS data in the FAA information system from which the data to be externally released originated; ensure sensitive NAS data is filtered from the data externally released; confirm compliance with relevant data protection policies; and/or ensure the authorization of the external release of sensitive NAS data, particularly SFD, is predicated on the data protections prescribed by Appendices H and I.

(2) Review the NDRB evaluation package, participate in NDRB discussions, and provide recommendations, including concurrence or non-concurrence and associated conditions, to the NDRB Secretariat for referral to the NDRB Chair for a final NDRB authorization decision.

(3) Be pre-designated as a primary and backup evaluator from the following FAA offices:

(a) **ATO System Operations Security (AJR-2)**. This evaluator advocates the SFD Security Program requirements and is the primary coordinator for NDRB engagement with the NDRB Ad Hoc Interagency Evaluators.

(b) **ATO Cybersecurity Group, Integration, Outreach, Planning Team (ACG/AJW-B450) Information Security and Data Protection Team (IS&DP).** This evaluator advocates the protection requirements for NAS STI and ATO CAVI data and the cybersecurity protection requirements for all SUI/CUI contained in FAA information systems containing NAS data. ACG Teams participating in the NDRB as board members can act as POCs for each other to ensure the NDRB receives the required input and signatures

(c) **ATO Cybersecurity Group, Cyber Engineering Team (ACG/AJW-B430)**. This evaluator represents the ATO CRB and provides linkage between NDRB processes and the "Authority to Operate" process for ATO information systems, including obtaining AO authorization for connections and a risk response for any proposed external release of sensitive NAS data, including required stipulations as appropriate. This evaluator also provides guidance to the NDRB on all FAA information systems containing NAS data. ACG Teams participating in the NDRB as board members can act as POCs for each other to ensure the NDRB receives the required input and signatures.

(d) **ATO NAS Defense Programs (NDP/AJW-B7)**. This is the FAA OPR for the dissemination of NAS data to Federal D/As and for the dissemination of NAS data from NDP-managed systems to SLTTLE agencies.

(e) **ATO Telecommunications Integrated Services Architecture Review Board (TIS ARB/AJM-5)**. This evaluator provides linkage between the NDRB processes and the approval processes for NAS data shared externally via FTI, inclusive of System Wide Information Management (SWIM) producers and non-SWIM connections, for both testing and operational configurations.

(f) **ATO NAS Configuration Control Board (NAS CCB/AJW-1810)**. This evaluator provides linkage between NDRB processes and the NCP process, inclusive of any direct connections to NAS equipment and information systems.

(g) **ATO NAS Systems Surveillance and Weather Support Team (AJW-1550)**. This evaluator provides linkage between the NDRB and AJW's field facilities, specifically the System Support Centers (SSC), for external release requests that involve physical connections between external equipment and FAA equipment.

(h) **Security and Hazardous Materials Safety (ASH), Office of Infrastructure Protection, Information Safeguards Division (AXF-200)**. This evaluator represents the OPR for FAA Order 1600.75 and provides guidance regarding the protection of SUI/CUI.

(i) **The Office of the Chief Counsel, Information, Data and Technology Law (AGC-400)**. This evaluator provides legal counsel to the NDRB and coordinates with other AGC offices, as needed. AGC-500 also provides direct support to the NDRB Secretariat for the

development and coordination of needed legal agreements between the FAA and External Recipients.

b. NDRB Ad Hoc Interagency Evaluators. The NDRB Secretariat will request the participation of the NDRB Ad Hoc Interagency Evaluators listed below in all Full NDRB Evaluations for Sensitive External Releases, which may affect relevant OPSEC, and other security equities of the participating Federal D/As. NDRB Ad Hoc Interagency Evaluators are required to:

(1) Be pre-designated as a primary and backup evaluator by the following Federal D/As: DoD, DHS, DOJ, and the Department of Energy (DOE). The NDRB Secretariat may request NDRB Ad Hoc Interagency Evaluators from additional Federal D/As, as needed.

(2) Characterize the OPSEC and other security risks posed by the external release to their parent D/A's activities in preliminary and final versions of *NAS Data External Release Interagency Security Risk Statement* (see Appendix I); identify possible security risk mitigations; and confirm the sufficiency of data protections imposed by the FAA in accordance with Appendices H and I.

(3) Review the NDRB evaluation package, participate in NDRB discussions, and provide recommendations, including concurrence or non-concurrence and associated conditions, to the NDRB Secretariat for referral to the NDRB Chair for a final NDRB authorization decision.

c. NDRB SME Participants. The NDRB Secretariat will request the participation of the NDRB SME Participants listed below in NDRB evaluations as needed.

(1) **ASH Advanced Threat Analysis and Mitigation Division (AXI-300)**. This participant will provide expert input pertaining to the identification, investigation, and analysis of threats to FAA employees, systems, and information. As necessary, AXI-300 provides threat analysis and recommended mitigations concerning a prospective External Recipient

(2) **Office of the Chief Data Officer (CDO/ADO-1)**. This participant will provide expert input on the FAA's enterprise data management guidance to the NDRB. In addition, CDO/ADO-1 provides technical expertise to System Owners and External Release Sponsors on compliance with the *OPEN Government Data Act.*

(3) **Other LOB/SO SMEs**. The NDRB Secretariat may invite other LOB/SOs to participate in NDRB evaluations as SMEs as needed.

7. INTEGRATION WITH THE AMS LIFECYCLE.

a. System Owners developing, acquiring, and sustaining FAA information systems that are designed to sustain a broadly shared release of NAS data outside of the FAA via one or more external connections established within its security authorization boundary, must consult jointly with the NDRB Secretariat and ACG/AJW-B4 in a timely manner for each AMS investment lifecycle phase (items 1-4 below) to mitigate scope, cost, and schedule risks. System Owners must use this joint consultation to integrate into their program plans, including budget, provisions supporting NDRB evaluation activity, compliance with SFD filtering, and other

conditions imposed by the NDRB, and implementation of Information System Security (ISS) requirements directed by ACG/AJW-B4, which are often related to NDRB approval conditions.

(1) **Concept and Requirements Definition (CRD)**: Prior to the completion of the Investment Initiative Provisional Security Category Table that lists all the information types contained in the system. Also reference the corresponding ISS assessment phase: ISS Risk Factors assessment.

(2) **Investment Analysis Readiness Decision (IARD)**: Prior to the completion of the Investment Initiative Security Category Table that lists all the information types contained in the system. SFD, NAS STI, and/or CAVI should be identified in the table by IARD. Also reference the corresponding ISS assessment phase: Preliminary ISS Assessment.

(3) **Initial Investment Decision (IID)**: Prior to the completion of the Investment Initiative Security Category Table that lists all the information types contained in the system. Information systems containing SFD, NAS STI, and/or CAVI must be categorized at the Moderate Confidentiality level as a minimum. Information systems containing SFD must describe how the system will implement AJR-2 authorized SFD filtering via system automation. Also reference the corresponding ISS assessment phase: Initial ISS Investment.

(4) **Final Investment Decision (FID)**: Prior to the completion of the Investment Initiative Security Category Table that lists all the information types contained in the system. System Owners must coordinate planned dates for testing and operational deployment with the NDRB Secretariat after FID is completed. Also reference the corresponding ISS assessment phase: Final ISS Investment.

NOTE –
System Owners may also be referred to the NDRB by the TIS ARB during one or more of the AMS investment lifecycle phases.

REFERENCES-
1. *Link to non-ATO ISS templates: https://fast.faa.gov/EMP_Information_Security_Assessment_Templates.cfm*

2. *Link to ATO ISS Procedures Guidance: ATO Information Systems Security Program | My FAA*

b. The System Owner must also coordinate with the NDRB Secretariat and ACG/AJW-B430 to ensure that sensitive NAS data (including SFD, NAS STI and ATO CAVI) when present in the system, is documented as specific information types in the information type table used by the Information System Security Assessment (ISSA) appropriate to individual phases of acquisition. If sensitive NAS data is present, the System Owner must implement Moderate Confidentiality information security controls at a minimum. If SFD specifically is present, the System Owner must implement SFD filtering authorized and validated by AJR-2 prior to operational deployment.

8. NDRB COORDINATION WITH ATO CRB, TIS ARB, AND NAS CCB.

The NDRB, the TIS ARB; the ATO CRB; and the NAS CCB have overlapping but distinct responsibilities with respect to: (1) the information types contained in the system; (2) the external connections contained in a system sourcing a Sustained External Release; and (3) the decision

document or action executed by each respective board. The NDRB Secretariat must synchronize the NDRB evaluations with these three other boards as outlined below:

a. NAS CCB. The NAS CCB evaluates NCPs to assess potential impact on the NAS. The NDRB Secretariat will participate in the NAS CCB as an evaluator, supporting the generation of Configuration Control Decisions (CCD) in response to NCPs involving external release of NAS data. The NDRB Secretariat will cooperate with the NAS CCB to support the completion of an NDRB Decision Record in advance of that Board's issuance of a NAS CCD involving overlapping NDRB and NAS CCB evaluations.

b. ATO CRB. ATO executes the cybersecurity risk management process mandated by FAA Order 1370.121 for ATO information systems through the ATO CRB. The NDRB Secretariat will participate in ATO CRB processes involving external release of NAS data and support risk acceptance by the ATO AO executed in the "Authority to Operate" or "ATO." The NDRB Secretariat will cooperate with the ATO CRB to support the completion of the NDRB Decision Record and AO risk response decisions, including required stipulations. Any relevant stipulations or other directive requirements made by the ATO AO must be included in the NDRB Decision Record as appropriate.

c. TIS ARB. The TIS ARB evaluates systems and external connections that utilize the FAA's FTI network. The TIS enables connections used to transmit NAS data externally in the testing environment at the FNTB located at WJHTCAA and the operational environment. The NDRB Secretariat will cooperate with the TIS ARB to support the completion of an NDRB Decision Record in advance of any external operational connection by the TIS. In addition, written NDRB approval must precede execution of any external test connection.

NOTE-
The information types contained in a system dictate which information security controls are required for the system. Information security requirements applicable to the confidentiality of the three ATO information types that qualify for protection as SUI/CUI, specifically SFD, NAS STI and ATO CAVI, are more rigorous than information security requirements to protect the confidentiality of non-sensitive NAS data.

9. PROCEDURES FOR ATO SYSTEM DISCONNECTS AND NAS DATA SUBSCRIPTION TERMINATIONS.

a. The FAA, in its sole discretion, may terminate an External Recipient's access to NAS data provided via an external connection for security reasons, inclusive of but not limited to the scenarios below.

(1) When the FAA determines the connection is not secure or that the connection poses an unacceptable security risk to FAA operations and assets, individuals, other organizations, or the United States; and

(2) When the FAA determines there is an issue with the External Recipient's need-to-know, duty-to-protect, or data protections supporting access to the released sensitive NAS data.

b. The NDRB will act to halt access by External Recipients to sensitive NAS data released by the FAA in cooperation, as appropriate, with the ATO AO, ATO Authorizing Official's Designated Representative (AODR), and ACG /AJW-B4 as outlined below:

(1) **Disconnect Memorandum.** The ATO AO has the authority to issue a disconnect memorandum requiring a System Owner to physically terminate a specified connection(s) to their system when significant security concerns with the connection have been identified and the associated risk cannot be mitigated to an acceptable level. When this security risk is identified as part of an NDRB evaluation, the NDRB Secretariat will forward the identified security issue to ACG/AJW-B4 and the ATO AODR for action.

(2) **NAS Data Access and/or Subscription Terminations.** When a security risk affecting an external release is identified by the NDRB Secretariat, NDRB evaluator, or ACG/AJW-B4, which after coordination with ACG is determined it cannot be mitigated to an acceptable level, the NDRB Chair will coordinate the issue of direction to the appropriate LOB/SO to terminate the user's access to sensitive NAS data.

NOTES-

1. *This procedure is separate from the normal administrative processes used by SWIM (for access to SWIM producers) and TFMS (for access to TSD Thin Client).*

2. *This procedure applies to instances where there is an existing administrative process to manage the initiation and termination of external user access to the NAS data that does not require physically shutting down the connection.*

This page left intentionally blank.

Appendix A. Acronyms

ADS-B	Automatic Dependent Surveillance - Broadcast
AO	Authorizing Official
API	Application Programming Interface
ARB	Architecture Review Board
ATC	Air Traffic Control
ATO	Air Traffic Organization
ATO CAVI	ATO Cybersecurity Authorization and Vulnerability Information
ATOP	Advanced Technologies and Oceanic Procedures
BVLOS	Beyond Visual Line-of-Sight
CCB	Configuration Control Board
CCD	Configuration Control Decision
CDM	Collaborative Decision Making
CFR	Code of Federal Regulations
CRB	Cybersecurity Review Board
CUI	Controlled Unclassified Information
DAA	Detect-and-Avoid
DoD	Department of Defense
DCRIT	Department of Defense Critical Infrastructure Security Information
EIM	Enterprise Information Management
ERAM	En Route Automation Modernization
FAA	Federal Aviation Administration
FFRDC	Federally Funded Research and Development Center
FLYR	Fly Reservations
FNTB	FAA National Test Bed
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSLTT	Federal, State, Local, Territorial, and Tribal
FTI	FAA Telecommunications Infrastructure
GBSS	Ground Based Surveillance Systems
GFI	Government Furnished Information
IE	Internet Enterprise
ISA	Interconnection Security Agreement
JMSDD	JAVA Messaging Service Description Document
LOB/SO	Line of Business/Staff Office
MOPS	Minimum Operational Performance Standards
MoSR	Mitigation of Sensitivity Risk

NAS STI	NAS Sensitive Technical Information
NCO	NAS Cyber Operations
NCR	NAS Common Reference
NCP	NAS Change Proposal
NDP	NAS Defense Programs
NDRB	NAS Data Release Board
NESG	NAS Enterprise Security Gateway
NIST	National Institute of Standards and Technology
NOP	National Offload Program
NOTAM	Notice to Airmen
OPIP	Operational Internet Protocol
OPSEC	Operations Security
OTA	Other Transaction Agreement
PDARS	Performance Data Analysis and Reporting
RAR	Risk Acceptance Report
SBS	Surveillance and Broadcast Services
SBSM	Surveillance Broadcast Service Monitor
SCM	Security Control Measures
SFD	Sensitive Flight Data
SFDPS	SWIM Flight Data Publication Service
SLTTLE	State, Local, Territorial, and Tribal Law Enforcement
SMS	Safety Management System
SRM	Safety Risk Management
SSI	Sensitive Security Information
SSP	System Security Plan
STDDS	SWIM Terminal Data Distribution System
STARS	Standard Terminal Automation Replacement System
SUI	Sensitive Unclassified Information
SWIM	System Wide Information Management
3PAO	Third Party Assessment Organization
TFM	Traffic Flow Management
TFMD	Traffic Flow Management Data
TFMS	Traffic Flow Management System
TIS	Telecommunications Integrated Services
UAS	Unmanned Aircraft System
U.S.C.	United States Code

NAS	National Airspace System

USS	UAS Service Supplier
WSDD	Web Service Description Document
WSRD	Web Service Requirements Document

Appendix B. Types of NAS Data and Related Definitions

Approved Domain Boundary Protection Gateway. A boundary system that separates security domains and protects an organization's systems and data. The NAS Enterprise Security Gateway (NESG) provides boundary protection for the entire NAS. An FAA-approved domain boundary protection gateway is the external side of the NESG, providing protection between NAS and non-NAS systems/networks.

ATO Cybersecurity Authorization and Vulnerability Information (ATO CAVI). Concerns system security measures and is largely generated as part of the process of conducting regular cybersecurity assessments and authorizations. In addition, ATO CAVI may reside in cybersecurity-related reports or presentations, other technical documentation, and in ATO repositories where these types of data are stored. ATO CAVI must be protected as SSI.

Collaborative Decision Making Program. A joint government/industry initiative aimed at improving air traffic flow management (ATFM) through increased information exchange among aviation community stakeholders. CDM is comprised of representatives from government, general aviation, airlines, private industry, and academia who work together to create technological and procedural solutions to the ATFM challenges faced by the NAS.

Controlled Unclassified Information (CUI). As defined by the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171, Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* CUI is any information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under EO 13526 or any predecessor or successor order, or Atomic Energy Act, as amended.

Efficiency-Critical NAS Service. Defined in the NAS Requirements Document 2013 (NAS RD 2013) as a key service that is used in the present operation of the NAS. Loss of an Efficiency-Critical Service has a major impact on the present operational capacity.

Essential NAS Service. Defined in the NAS RD 2013 as a service that, if lost, would significantly raise the risk associated with providing safe and efficient NAS operations.

External Connection. Defined by this order as a connection from a non-FAA entity to an FAA information system and/or connection point for the purpose of FAA sharing real-time or near real-time NAS data with an External Recipient.

NOTE-
Other FAA LOBs/SO use the term "external" to mean outside the system and/or outside the information security domain, but still internal to the FAA.

External Recipient. Term of art used by this order to denote a non-FAA, non-Federal D/A entity, which has either been authorized by the FAA to access NAS data or is involved with a proposed access being evaluated by the NDRB or otherwise addressed by the NDRB Secretariat.

External Information System. An information system belonging to and/or managed by a non-FAA entity.

External Release of NAS Data. Defined by this order as the release of NAS data to entities outside the FAA.

NOTES-
1. *Contract support for FAA programs, information systems, second-level engineering, operations support, and information security is generally considered to be internal NAS data sharing (see policy exception in Chapter 2, para 3d, of this order). Contract support access to sensitive NAS data is authorized when the sensitive NAS data is identified as GFI necessary for the performance of the contract.*

2. *NAS data sharing between FAA information security domains, such as the NAS OPIP environment and the Mission Support operating environment (as defined by FAA Order 1370.121), is considered to be internal NAS data sharing and not under the purview of this order.*

External Release Sponsor. Term of art used by this order to denote the FAA office serving as the primary advocate for an external release of NAS data undergoing NDRB evaluation. The External Release Sponsor is responsible for a broad range of tasks integral to the NDRB evaluation process. This could include requirements related to: documentation and other artifacts; discussions with the NDRB evaluators; legal agreements; funding; and, for external releases of sensitive NAS data, need-to-know, duty-to-protect, and data protection.

NOTES-
1. *The roles of the External Release Sponsor and the System Owner may be carried out by the same office.*

2. *The External Release Sponsor will typically collaborate with the External Recipient throughout the NDRB evaluation process.*

FAA Field Facilities. For purposes of this order, FAA field facilities include ATC facilities, Technical Operations facilities, MMAC, WJHTCAA, ATL and STL IESP, OKV, and other data centers.

Filtered NAS Data. NAS data that has been filtered via a software process to remove *all* SFD. The filtering software process accomplishes this by identifying and marking a flight as either SFD or non-sensitive so that *all* data elements associated with an SFD flight are removed from the filtered NAS data set. SFD contains multiple types of SUI/CUI. The term “filtered NAS data” only applies to SFD.

Filtering. A process specific for SFD, implemented via software and “filter files” maintained by FAA System Operations Security, by which SFD can be identified, marked, and removed from a NAS data set or NAS data feed. NAS Data that has been filtered does not contain SFD. The term filtering applies only to SFD.

Focused External Release. Term of art used by this order to denote the external releases of NAS data that meet the following criteria: the released NAS data is non-sensitive; the released NAS data is sourced by an FAA information system, which is not designed to broadly share NAS data outside and does not incorporate external connections established within its security authorization boundary; and the release is intended to be temporary, specific to an activity with a planned end.

NOTE –
The information systems sourcing data for Focused External Release are generally engineered for only internal FAA use. Some of these systems may include external connections within their security authorization documentation boundary, but none of those external connections is designed to broadly share NAS data with the public. Examples

of these systems include Surveillance and Broadcast Services (SBS), which contains Automatic Dependent Surveillance Broadcast (ADS-B) data; SBS Monitor (SBSM); Performance Data Analysis and Reporting System (PDARS); En Route Automation Modernization system (ERAM); and Standard Terminal Automation Replacement System (STARS).

Full NDRB Evaluation. Comprehensive NDRB evaluations of external releases, which are generally characterized as: addressing novel proposals for external release; requiring participation of all pre-designated NDRB evaluators; and producing an NDRB Decision Record. See Chapter 3, paragraph 3, for a more detailed definition.

Historical NAS Data. NAS data with a time component, such as NAS surveillance or ATC automation data, that is provided via a delayed means (other than as a real-time or near real-time NAS data feed) through a secure external connection or other secure dissemination method, as applicable, is considered historical NAS data.

NOTE-
This definition does not apply to new requests by a single entity for access to non-sensitive NAS data authorized for release via an NDRB Decision Record (i.e., a new SWIM onboarding request for access to filtered TFMS data).

System Owner. An FAA office formally responsible for the development and sustainment of an FAA information system containing NAS data that sources an external release.

Interconnection Security Agreement (ISA). A document that specifies the technical and security requirements for establishing, operating, and maintaining an interconnection between two or more systems. The ISA also supports an overarching legal agreement, such as an OTA between the organizations. The ISA typically includes the following: documentation of the requirements for connecting the systems; a description of the mandated protection requirements and controls, including SCM provisions, necessary to protect exchanged information and the systems processing, storing, or transmitting the information; MoSR provisions implemented by FAA; a topological drawing of the interconnection; and a signature line for participating organizations. An ISA is indicated when the information exchange occurs via an interconnection.

Key Site Testing. Testing conducted at one or more FAA operational facilities to verify system performance and to ensure the system is ready for installation at the remaining operational sites.

Mitigation of Sensitivity Risk (MoSR). Denotes the structured set of redactions implemented by the FAA on releases of NAS surveillance and other NAS data containing SFD and other SUI/CUI to external non-Federal entities in accordance with the procedures in Appendix G and Appendix H. MoSR provisions are intended to mitigate the risk posed to security interests of unauthorized access to SUI/CUI released by the FAA despite implemented data protections. MoSR provisions focus on moderating impacts on the OPSEC-sensitive government missions conducted by DoD, DHS, DOJ, and DOE, as well as other FSLTT D/As responsible for national defense, homeland security, or law enforcement missions. These mitigations will typically include: the removal or modification of select data elements of particular security sensitivity; tailored surveillance service volumes; and limits on the sharing of surveillance system performance characteristics.

NOTE-

MoSR provisions are implemented by the FAA on the FAA side of the data stream. MoSR provisions are not implemented by the external requestor. MoSR provisions are generally applicable only to a proposed release that involves NAS radar data.

NAS Data and Information. The data and information from the U.S. aviation ecosystem; ATC automation, surveillance, navigation, communication, weather, maintenance and operational support equipment and services; air navigation facilities; airports or landing areas; aeronautical charts, information and services; rules, regulations and procedures, technical information, and manpower and material directly used to ensure safe and efficient use of U.S. navigable airspace. Included is data from components shared jointly with the military and other governmental entities and data from support environments such as training, development, testing, and security (physical, personnel, and cyber). NAS data is generated in the NAS, but may exist in any environment (NAS Operations, NAS Support, R&D, Mission Support, or external requestor domains, such as other government agencies, aviation partners, academia, and industry). It maintains its designation as NAS data regardless of the environment in which it resides, and this designation determines the requirements for its protection, handling, and sharing.

NOTE-
NAS data was initially defined in the Notice for Data and Information Distribution Policy, published in 79 Fed. Reg., 76438, December 22, 2014, and was further refined to the definition cited above in FAA Order 1375.1, Data and Information Management Policy.

NAS Sensitive Technical Information (STI). Information (inclusive of the data elements it comprises) of a technical nature used in operation or support of the NAS, which an adversary might be able to use or leverage, alone or in conjunction with other information, to compromise, disrupt, or interfere with the NAS, any NAS service, or NAS asset. It includes information essential to the design, development, production, operation, application, maintenance, or support of a NAS asset. NAS STI may be found in manuals, publications, specifications, standards, plans, photographs or videos, detailed technical descriptions, or procedures, change proposals, data sets, studies, Safety Risk Management (SRM) documentation, test reports, and analyses that may reveal the "as built" or planned nature and details of NAS networks, systems, subsystems, and components. Material containing NAS STI may exist in any media form and in any physical location. It may be stored on any network, including the Mission Support network as well as R&D networks (e.g., LabNet, NAS Prototyping Network). NAS STI may also be found in non-NAS systems or assets. This definition is applicable to operational, support, administrative, research, development, demonstration, test, training, laboratory, cloud, vendor, contractor, Federally Funded Research and Development Center (FFRDC), academic, and any other environment where this information may be stored, processed, or transmitted. NAS STI must be protected as SSI. See ACG Guidance, *Identifying National Airspace System (NAS) Sensitive Technical Information (STI).*

NDRB Evaluator. Cadre of pre-designated NDRB evaluators from a mix of AJR, AJW, AJM, ASH, and AGC offices who will be, as a default, requested by the NDRB Secretariat to participate in all Full NDRB Evaluations.

NDRB Ad Hoc Interagency Evaluator. Cadre of NDRB evaluators from select Federal D/As with OPSEC and other security interests that could be directly affected by the external release of sensitive NAS data. Evaluators of this type are pre-designated to represent DoD, DHS, DOJ, and DOE.

NDRB SME Participants. SMEs invited by the NDRB Secretariat to provide expert technical input to NDRB evaluation deliberations but will not be asked to provide authorization recommendations.

Near Real-Time NAS Data. Any NAS data processed by an FAA information system that is not intentionally delayed from its original structure and/or process and which is then provided via a secure external connection. Near real-time NAS data does not meet FAA requirements for the provision of safety-critical services such as the separation of crewed aircraft.

Nonpublic NAS Data. NAS data that may not be made available to the public for privacy, security, confidentiality, regulation, or other reasons as determined by law. The *OPEN Government Data Act* requires Federal agencies to identify all of their nonpublic data assets.

Open Government Data Asset. Per the *OPEN Government Data Act*, this is a data set maintained by the Federal government that is machine-readable, available in open format, not encumbered by restrictions that would impede its use or reuse, and based on an underlying open standard, maintained by a standards organization. The Act requires Federal agencies to identify all of their open government data assets.

Operations Security (OPSEC). A security discipline designed to deny adversaries the ability to collect, analyze, and exploit information that might provide an advantage against the United States by preventing inadvertent compromise of *critical information* through a process of continual assessment that identifies and analyzes *critical information,* vulnerabilities, risks, and external threats.

NOTES-

1. *Critical Information is defined in NSPM-28 as classified or unclassified information important to the achievement of United States objectives and missions that requires safeguarding or dissemination controls and for which unauthorized access to or modification of, could adversely affect the national interest or national security, the conduct of Federal programs or operations, or individual privacy and identity management, and which may be of use to an adversary of the United States.*

2. *SFD has been identified as critical information by national security executive branch agencies and organizations representing SLTTLEs. The ATO System Operations Security SFD Security Program provides OPSEC support to these agencies.*

Other Transaction Agreement (OTA). As referenced in Public Law 104-264, October 9, 1996, an OTA is a transaction that does not fall into the category of procurement contracts, grants, or cooperative agreements.

Pilot-Dispatch Interface System. An FAA information system engineered to share specific NAS data directly via a unicast or one-to-one connection with certain NAS users, specifically pilots, aircraft owners, fractional owners, and/or flight dispatch organizations. A pilot-dispatch interface system is *not* engineered to share any data from its system with the public. Pilot-dispatch interface systems include data link communication systems such as Tower Data Link Services (TDLS) System, as well as NAS access web platforms such as Fly Reservation (FLYR) and ADAPT. Flight dispatch organizations consist of Airline Operations Centers (AOCs), military flight dispatch units, and civilian flight dispatch organizations that are also CDM members.

Proprietary NAS Data. Any NAS data relating to, or associated with, a company's products, business, or activities, including, but not limited to, trade secrets; product research and development; and existing and future product designs and performance specifications. Proprietary NAS data may be exempt from public release under FOIA, Exemption 4.

Public Data Asset. A data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under FOIA.

Public NAS Data. A NAS data asset maintained by the FAA that may be released to the public, has been released to the public in an open format and is discoverable through a search of Data.gov or any successor to Data.gov, or is part of the worldwide public domain, or, if necessary, published with an open license. The *OPEN Government Data Act* requires Federal agencies to identify public data assets.

Real-Time NAS Data. NAS data provided via an adapted secure external connection that is engineered by the FAA to support the provision of safety-critical NAS services (e.g., ATC separation services provided by DoD). Note: Provision of real-time NAS data requires FAA NDP sponsorship of the requesting DoD unit and adaptation of the NAS data feed to the DoD site (i.e., a STARS feed to a DoD ATC facility), into the NAS via the NAS CCB process.

NOTE-
See below for the definition of "safety-critical."

Redacted NAS Data. Denotes sensitive NAS data that has been modified to redact, remove, or otherwise withhold NAS STI and ATO CAVI from unauthorized release. Redacted NAS data can also denote the modification of sensitive NAS data, particularly including NAS surveillance data, to execute a MoSR.

NOTE-
Redaction may be a manual process but can also be implemented via software in situations where SUI/CUI data elements remain in the data set, either by FAA design, and/or by limitation of the data set (i.e., not enough data elements for SFD filtering to work correctly).

Safety-Critical. A key NAS service in the protection of human life. Loss of a safety-critical service increases the risk of loss of human life.

REFERENCE-
National Airspace System Requirements Document, NAS-RD-2013, dated August 11, 2014.

Sanitized NAS Data. NAS data that has been significantly altered to the point where AXF-200 determines that SUI/CUI is no longer present in the NAS data set. In general, the provision of a sanitized NAS data set is only possible for historical NAS data.

EXAMPLE-
NAS primary radar data with the time and date altered, location altered, and plot position data rotated over 120 degrees from the actual plot positions still contains the plot/track position data element, which is normally considered SFD. In this example, the data was altered sufficiently for AXF-200 to determine that SUI/CUI was no longer present in the data set, which allowed it to be shared with the sponsored external requestors.

Security Control Measures (SCM). Denotes the structured set of cyber, physical, and personnel security requirements imposed by the FAA on releases of NAS data containing SFD and other SUI/CUI to external non-Federal entities in accordance with the procedures in Appendix H and Appendix I. These release-specific requirements comply with FAA Orders 1600.75, *Protecting Sensitive Unclassified Information (SUI)*, and 1370.121, *FAA Information Security and Privacy: Policy*, and are built on the requirements prescribed by the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

Sensitive Flight Data (SFD). ***All*** flight data related to an individual flight, inclusive of positional, track and identification data (e.g., call sign, aircraft registration number, aircraft type, beacon code, route of flight) about or associated with a U.S. sensitive government mission conducted for the purposes of national defense, homeland security, intelligence, or law enforcement. SFD that the FAA possesses on sensitive government missions is protected as SUI/CUI and not released to the public. SFD exists in any FAA information system or data set that contains information or data on individual flights, inclusive of real-time NAS data and historical data. SFD is also a specific information security information type used by the FAA that must be protected at least at the moderate confidentiality impact level, in accordance with applicable Federal information security requirements for SUI/CUI contained in FAA Order 1370.121 and FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI)*.

NOTES-

1. *The FAA cannot ensure protection of any flight data transmitted from aircraft by ADS-B Out or other open and unencrypted avionics equipment as this data is also collected by third parties. Flight data collected directly from aircraft by third parties is not protected by the FAA.*

2. *Not all flight data is considered SFD. FAA information systems or data sets that contain information or data on individual flights have a mix of non-SFD and SFD. Only those flights identified as SFD via the authoritative AJR-2 filter file process are protected as SUI/CUI.*

3. *SFD has been identified as critical information by national security executive branch agencies and organizations representing SLTTLE agencies as part of their respective OPSEC programs. FAA provides OPSEC support to these agencies by protecting SFD via the ATO System Operations Security SFD Security Program and by ensuring there is no unauthorized disclosure of SFD to external entities via the provisions in this order.*

4. *SFD comprises DCRIT, SSI, and FOUO data. Both DCRIT and SSI are categories of CUI, a U.S. Government-wide program for managing unclassified information that requires safeguarding or dissemination controls established by EO 13556, Controlled Unclassified Information, and is governed by 32 CFR Part 2002, Controlled Unclassified Information. At the time of the publication of this Order, the FAA had not yet fully implemented CUI. This Order focuses on data protection requirements mandated by the FAA's SUI/CUI program but is also informed by CUI-related requirements regarding the protection of SFD's DCIT and SSI elements.*

Sensitive Flight Data (SFD) Security Program. The program that administers FAA security measures designed to support OPSEC for sensitive government missions. The SFD Security Program has two major components, protective security measures the FAA implements and preventative security measures, such as tactics, techniques, and procedures (TTPs) the FAA recommends other agencies take (also known as OPSEC recommendations). The FAA can only protect SFD in data that originates within the FAA.

Sensitive NAS Data. For purposes of this order, the term "sensitive NAS data" means NAS data containing one or more types of SUI/CUI.

Sensitive Unclassified Information (SUI). As defined in FAA Order 1600.75, SUI is unclassified information in any form, including print, electronic, visual, or aural forms, that must be protected from uncontrolled release to persons outside the FAA and indiscriminate dissemination within the FAA. It includes aviation security, homeland security, and protected critical infrastructure information. SUI may include information that may qualify for withholding from the public under FOIA, including under Exemption 3, which protects information under specific statutes like SSI and DCRIT, and/or Exemption 7(E) for law enforcement techniques like sensitive flight data.

Static NAS Data. NAS data in the form of documentation, such as, but not limited to, technical manuals, service description documents, service requirements documents, security documents, security assessment documentation, NCPs, and interface documents.

Streaming NAS Data. Either real-time or near-real time NAS data that is provided to the requestor via a machine-to-machine connection. Requests for access to non-sensitive streaming NAS data approved for external release via an NDRB Decision Record can be processed without an end date. Requests for access to streaming NAS data that contains SUI/CUI are processed with an end date linked to the expiration date on the legally binding agreements that establish duty-to-protect.

SUI-Authorized Persons. In the context of external release requests handled in accordance with the procedures in Appendix I, "SUI-authorized persons" are those personnel employed by the external requestor or by its contractors (and sub-contractors) and other cooperating entities requiring access to the FAA-provided SFD or other SUI/CUI and subject to legally binding agreements between the requestor and the FAA governing the release and the related data protection requirements prescribed by the FAA.

Sustained External Release. External releases of NAS data, which meet the following criteria: the released NAS data is non-sensitive (i.e., does not contain SUI/CUI or nonpublic information); the released NAS data is sourced by an FAA information system, which is designed to broadly share NAS data outside of the FAA via one or more external connections established within its security authorization boundary; and the release is intended to be sustained (i.e., has no planned end).

NOTES –

1. *The aforementioned systems include SWIM producers (systems designed to share NAS data via external SWIM connections) and systems with legacy connections (such as Traffic Situation Display [TSD] Thin Client) to external entities.*

2. *This definition does not generally apply to situations where FAA shares sensitive NAS data via a dedicated connection with a trusted international partner (e.g., sharing ERAM data with NAV CANADA); to DoD (e.g., STARS data) for the purpose of providing ATC services; or to Federal D/As for security and law enforcement purposes (e.g., sharing NAS radar data with DoD and DHS). These external release cases are generally covered by one or more of the exceptions listed in Chapter 2, paragraph 3.*

System. Consistent with FAA Order 1370.121, *FAA Information Security and Privacy: Policy,* and supplemental implementation directives, the term "system" refers to an assembly of computer hardware (e.g., sub-networks, application servers, file servers, workstations, data, etc.) and/or application software configured for the purpose of processing, handling, storing, transmitting, and receiving data, which is used in a production or support environment to sustain

specific applications and business organizations in their performance of tasks and business processes.

Targeted NDRB Evaluation. Expedited, narrowly scoped NDRB evaluations of external releases, which are generally characterized as: addressing external releases previously approved by an NDRB Decision Record; only necessitate the participation of a limited set of NDRB evaluators; and produce an NDRB Administrative Record. See Chapter 3, paragraph 3, for a more detailed definition.

Third-Party Service Supplier. An entity other than the FAA that provides a distributed service that affects the safety or efficiency of the national airspace system, including UAS service suppliers, supplemental data service providers, and infrastructure providers, such as providers of ground-based surveillance, command-and-control, and information exchange to another party.

Unfiltered NAS Data. NAS data that contains one or more sensitive NAS data elements qualified as SFD, NAS STI, or ATO CAVI. In the context of this order, "unfiltered NAS data" most often refers to NAS data containing unmarked SUI/CUI, specifically including SFD.

Appendix C. Related Directives, Publications, and Documents

- 49 U.S.C. 106, *Federal Aviation Administration*
- 49 U.S.C. Subtitle VII, *Aviation Programs*
- 10 U.S.C. 130e, *Treatment Under Freedom of Information Act of Certain Critical Infrastructure Security Information*
- 49 U.S.C. 114, *Transportation Security Administration*
- 5 U.S.C. 552, *Public information; agency rules, opinions, orders, records, and proceedings*
- 44 U.S.C. Chapter 35, *Coordination of Federal Information Policy, Subchapter I, Federal Information Policy Executive Order (EO) 14028 - Improving the Nation's Cybersecurity*
- Executive Order (EO) 13556, *Controlled Unclassified Information*
- National Security Presidential Memorandum (NSPM-28), *The National Operations Security Program*
- 32 CFR 2002, *Controlled Unclassified Information (CUI)*
- 49 CFR 1520, *Sensitive Security Information*
- Federal Information Processing Standards Publication (FIPS) 140-2, *Security Requirements for Cryptographic Modules*; FIPS 199, Standards for Security Categorization of Federal Information and Information Systems; and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations; 800-147, *Basic Input/Output System (BIOS) Protection Guidelines*; 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*; and 800-172, Enhanced *Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*
- FAA Order 1600.75, *Protecting Sensitive Unclassified Information (SUI)*
- FAA Order 1370.121, *FAA Information Security and Privacy: Policy (and its supplemental implementing directives)*
- FAA Order 1370.130, *Air Traffic Organization (ATO) Cybersecurity Roles and Responsibilities*
- FAA Order 1375.1, *Data and Information Management Policy*
- FAA Order 1800.66, *Configuration Management Policy*
- FAA Order JO 7110.67, *Air Traffic Management Security Procedures and Requirements for Special Operations*

Appendix D. NDRB Forms and Applications

FIG D-1. FAA Form 1200-5, NAS Data Release Request

NAS Data Release Request **OMB Approved 2120-0668**
11/30/2024

Paperwork Reduction Act Statement: This data is collected to assess the validity of your request for approval/disapproval. It will take approximately 1 hour to complete this form. The collection is mandatory, and all information collected shall be kept confidential. An agency may not collect, and a person is not required to respond to an information collection, unless it displays a currently valid OMB Control Number. Comments concerning the accuracy of this burden and suggestions for reducing the burden should be directed to the FAA at: 800 Independence Ave SW, Washington, DC 20591, Attn: Information Collection Clearance Officer, ABA-20

1. Business/Organization Name		2. Business Phone Number
3. Address *(Street, City, State, ZIP Code)*		
4. Point of Contact (POC) Name	5. Phone Number	6. Full E-mail address

7. Are you currently receiving NAS data? Yes ☐ No *(If no, skip to #10)*

8. Indicate your authority to access NAS data: ☐ Memorandum of Agreement ☐ Government contract ☐ Other *(Explain)* *(Attach documentation)*

9. Indicate if you have an approved NCP(s) on file: ☐ Yes ☐ No If yes, list the case file number(s):

10a. Type of data you are requesting: ☐ Delayed ☐ Recorded 10b. Describe the data requested: *(Attach additional sheets)*

11. Describe your proposed method for acquiring data: *(Attach additional sheets)*

12. Describe the nature of your organization/business and the purpose for this request. *(Attach additional sheets)*

13. Describe your sensitive data filtering process. *(Attach additional sheets)*

14. List any non- U.S. citizen personnel you will employ for this data request. Explain his/her duties in relation to this data request. *(Attach additional sheets)*

FOR OFFICE USE ONLY: Request Date: ____/____/____ **Package Date:** ____/____/____

(FAA FORM 1200-5) (2-02) Local Reproduction Authorized NSN: 0052-00-923-3000

Instructions for FAA Form 1200-5

If you require additional space to provide your answers, write them on a separate sheet preceded by the item number and attach them to this request.

1. Enter the complete registered name of the business or organization that has authority for all operations.
2. Enter the phone number of the business or organization.
3. Enter the complete address of the business or organization.
4. Enter the Point of Contact (POC) who will have the delegated authority. If this person is the same as the one stated in 3, indicate by entering "same as above."
5. Enter the phone number of the POC. If this person is the same as the one stated in item 4, indicate by entering "same as above."
6. Enter the business or organization's e-mail address.
7. Check the appropriate box. If the answer is "Yes," attach a copy of the appropriate documentation.
8. Check the appropriate box.
9. Indicate whether or not you have an approved NAS Change Proposal (NCP) with the FAA and include that number. If you have more than one NCP, list all NCP numbers.
10. Describe the type of data you are requesting – location, facility, exact data sought. Be as specific as possible.
11. Describe your method for accessing NAS data. Tell what your equipment will do, how it will operate, the method of filtering, and any other capabilities as required.
12. State the type of business you operate and the specific purpose for using the NAS data.
13. List, in specific detail, your filtering process and data safeguard procedures.
14. Provide the names of any non-U.S. citizen personnel you plan to employ for this data request, along with the scope and nature of work the individual will perform.

NOTES –

1. *For more information on Data Management, view FAQs here:*
https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/perf_analysis/faq/

2. *The official FAA NAS Data Release Request Form 1200-5 is found here:*
https://www.faa.gov/documentLibrary/media/Form/FAA_Form_1200-5_Exp_11_30_2024.pdf

Appendix E. Sustained External Release

1. APPLICATION.

a. The procedures prescribed by this Appendix apply to external releases of NAS data that meet the following criteria: the released NAS data is non-sensitive (i.e., does not contain SUI/CUI or nonpublic information); the released NAS data is sourced by an FAA information system, which is designed to broadly share NAS data outside of the FAA via one or more external connections established within its security authorization boundary; and the release is intended to be sustained (i.e., has no planned end).

b. The procedures below are specific to Sustained External Release and complement the procedures articulated in Chapter 3 of this order, which are common to all categories of external release.

2. TAILORED TRIGGERS FOR FULL AND TARGETED NDRB EVALUATIONS.

In addition to the basic criteria and characteristics for NDRB evaluations cited by Chapter 3, paragraphs 2 and 3 of this order, the NDRB Secretariat will use the tailored triggers indicated below to initiate Full and Targeted NDRB evaluations for Sustained External Release cases.

a. Full NDRB Evaluation. Evaluations of this type will be initiated if one or more of the criteria listed below are met in a manner implicating a Sustained External Release and affecting the source information system or the release itself:

(1) An FAA information system is approved for operational deployment, which includes one or more NCPs to establish a new external data or information message service(s).

(2) A new data or information message service is created, or a new data message or NAS data element is added to an existing data or information message service, when the change involves sharing or withholding data from the public and has not been previously approved by the NDRB.

NOTE –
For changes where there is a need to withhold the data or information message service from external release previously approved by an NDRB Decision Record, a targeted NDRB evaluation may be sufficient.

(3) The use of a new external connection type and/or mechanism (e.g., new FAA Application Programming Interface [API] connection) is proposed when the change affects external data sharing and has not been previously approved by the NDRB.

EXAMPLE-
The SWIM Terminal Data Distribution System (STDDS) has existing NDRB authorization to release filtered NAS data over the SWIM NESG connection and the SWIM Cloud Distribution Service (SCDS). However, the STDDS program office must request NDRB approval to release filtered STDDS from the Enterprise Information Management (EIM) platform to one or more external entities via an FAA API. In this example, the STDDS program office is the System Owner and External Release Sponsor and is responsible for adjudicating external requests for access to STDDS data in accordance with the conditions prescribed by the authorizing NDRB Decision Record. In this example, the EIM program office does not automatically share these responsibilities unless a specific arrangement is made with the STDDS program office and NDRB Secretariat.

(4) A major system release or automation update is proposed for an FAA information system that contains SFD or other SUI/CUI; is experiencing ongoing SUI/CUI spillage to unauthorized external entities; and has not submitted a written SUI/CUI protection mitigation plan to the NDRB Secretariat.

NOTE-
After the written SUI/CUI protection mitigation plan has been submitted to the NDRB Secretariat, the system only needs to undergo a Full NDRB evaluation when one of the other triggering events in this section applies. The system will also need to undergo periodic Targeted NDRB evaluations as outlined in paragraph c below until the SUI/CUI spillage is fully mitigated.

b. Targeted NDRB Evaluation. Evaluations of this type will be initiated if one or more of the criteria listed below are met in a manner implicating a Sustained External Release and affecting the source information system or the release itself:

(1) Regression testing is being conducted for a change to a system, which could affect its external release and functionality of existing SFD filtering.

NOTE-
Checks to determine if SFD filtering is functioning properly can be accomplished via SFD filtering validation and/or SFD filtering regression testing. These checks must be scheduled prior to any external sharing of NAS data related to other testing activities.

(2) A major system release or automation update is proposed for an FAA information system, which: contains SFD or other SUI/CUI; is experiencing ongoing SUI/CUI spillage to unauthorized external entities; and has submitted a written SUI/CUI protection mitigation plan to the NDRB Secretariat.

(3) Testing activities are proposed to support the initial deployment of a new information system or subsequent operational releases of an existing information system.

NOTE –
In some cases, this NDRB evaluation activity may coincide with the SFD filtering validation and/or SFD regression testing. SFD filtering validation and/or SFD filtering regression testing must be scheduled well ahead of planned external sharing of NAS data.

(4) An FAA information system that has implemented SFD filtering, makes one or more changes to the originating system's SFD filtering software or algorithm affecting the external release of its data previously approved by the NDRB.

(5) There is a need to constrain a new or modified data or information message service from external release previously approved by the NDRB.

NOTE –
In this case, the NDRB may decide to issue a new NDRB Decision Record, which will state that the new or modified data or information service is not approved to release NAS data externally.

3. TAILORED NDRB EVALUATION PROCEDURES.

In addition to the common procedures for NDRB procedures cited by Chapter 3 of this order, the NDRB Secretariat will ensure the following procedures specific to Sustained External Release cases are implemented.

a. Pre-Coordination. The NDRB Secretariat must cooperate with the System Owner, External Release Sponsor, and SFD Security Program Manager to carry out the following pre-coordination tasks before the NDRB evaluation is started:

(1) Analyze the composition of the data set and determine whether the data source system contains any SUI/CUI including SFD, and NAS STI.

(2) Consider whether the data set contains any potential proprietary or other nonpublic NAS information that requires protection.

(3) If SFD or NAS STI are present, develop an SFD filtering mechanism (e.g., software or algorithm) and comparable capabilities for NAS STI to be incorporated into the subject information system or an external connection tailored to remove the sensitive NAS data from sustained external release.

(4) Ensure any required coordination with the NAS CCB, ATO CRB, and TIS ARB is synchronized with the planned NDRB evaluation as prescribed by the procedures in Chapter 3, paragraph 8.

(5) Develop an NDRB evaluation plan specific to the case being discussed, including: timelines and milestones; requirements for the submission of documents and other artifacts; and required actions to be completed by the System Owner and External Release Sponsor.

b. Evaluation. The NDRB Secretariat and NDRB evaluators must cooperate with the System Owner and External Release Sponsor to carry out the following tasks as part of the NDRB evaluation planned during pre-coordination:

(1) Validate that the System Owner has successfully incorporated effective filtering mechanisms for SFD, and redaction, removal, or otherwise withholding of NAS STI and ATO CAVI from the subject system and/or external connection.

(2) Characterize the ability of the System Owner and External Release Sponsor to implement effective filtering, including an examination of timing relative to program milestones and deficiencies. And use this information to support the production of, if needed, a corrective POAM by the System Owner.

(3) Incorporate into the NDRB Decision Record or NDRB Administrative Record conditions that specify how the System Owner and External Release Sponsor must maintain and verify the effectiveness of the filtering solution developed and implemented for the NDRB evaluation into the future.

Appendix F. Focused External Release

1. APPLICATION.

a. The procedures prescribed by this Appendix apply to external releases of NAS data that meet the following criteria: the released NAS data is non-sensitive; the released NAS data is sourced by an FAA information system, which is not designed to broadly share NAS data outside and does not incorporate external connections established within its security authorization boundary; and the release is intended to be temporary, specific to an activity with a planned end.

b. The procedures below are specific to Focused External Release and complement the procedures articulated in Chapter 3 of this order, which are common to all categories of external release.

2. TAILORED TRIGGERS FOR FULL AND TARGETED NDRB EVALUATIONS.

In addition to the basic criteria and characteristics for NDRB evaluations cited by Chapter 3, paragraphs 2 and 3 of this order, the NDRB Secretariat will use the tailored triggers indicated below to initiate Full and Targeted NDRB evaluations for Focused External Release cases.

a. Full NDRB Evaluation. Evaluations of this type will be initiated if one or more of the criteria listed below are met in a manner implicating a Focused External Release, and affecting the source information system or the release itself:

(1) A System Owner and/or External Release Sponsor proposes to initiate a novel external release that has not been evaluated and authorized by the NDRB previously.

(2) New NAS data elements that contain SUI/CUI, have been added to an information system, from which external releases have been made in the past as authorized by an existing NDRB Decision Record, and when the System Owner desires to retain the option for future external releases.

b. Targeted NDRB Evaluation. Evaluations of this type will be initiated if one or more of the criteria listed below are met in a manner implicating a Focused External Release and affecting the source information system or the release itself:

(1) An information system containing SFD, from which external releases have been made in the past as authorized by an existing NDRB Decision Record, is proposing to change its SFD filtering software and/or algorithm.

(2) An FAA information system plans to share NAS data externally during testing at the FNTB located at WJHTCAA or during other FAA testing activities.

3. TAILORED NDRB EVALUATION PROCEDURES.

In addition to the common procedures for NDRB procedures cited by Chapter 3 of this order, the NDRB Secretariat will ensure the following procedures specific to Focused External Release cases are implemented.

a. Pre-coordination. The NDRB Secretariat must cooperate with the System Owner, External Release Sponsor, and SFD Security Program Manager to carry out the following pre-coordination tasks before the NDRB evaluation is started:

(1) Ensure the External Release Sponsor submits an FAA Form 1200-5 to the NDRB Secretariat at 9-AJR-NDRB-Executive-Secretariat@faa.gov.

(2) Analyze the composition of the data set and determine whether the data source system contains any SUI/CUI, including SFD, NAS STI, and ATO CAVI.

(3) Consider whether the data set contains any potential proprietary or other nonpublic NAS information that requires protection.

(4) If SFD, , NAS STI, or ATO CAVI are present, develop an SFD filtering mechanism (e.g., software or algorithm) and comparable capabilities (i.e., redaction, removal, or otherwise withholding) for NAS STI and ATO CAVI to be applied as: an ad hoc, one-time solution to the external release to be evaluated; or as a maintained capability for future, comparable external releases.

(5) Characterize the proposed external release, including: defining what data is to be released (e.g., historical or near real-time); determining the frequency and duration of the release; and specifying the external connection type and/or other mechanism (e.g., one-time data transfer).

(6) Ensure any required coordination with the NAS CCB, ATO CRB, and TIS ARB is completed as prescribed by the procedures provided in Chapter 3, Section 8.

(7) Develop an NDRB evaluation plan specific to the case being discussed, including: timelines and milestones; requirements for the submission of documents and other artifacts; and required actions to be completed by the System Owner, External Release Sponsor, and, in select cases, the External Recipient.

b. Evaluation. The NDRB Secretariat and NDRB Evaluators must cooperate with the System Owner, External Release Sponsor, and, as needed, External Recipient to carry out the following tasks as part of the NDRB evaluation planned during pre-coordination:

(1) Validate that the System Owner has successfully filtered SFD, or redacted, removed, or otherwise withheld NAS STI and ATO CAVI, from the planned external release as an ad hoc, one-shot solution.

(2) Characterize the ability of the System Owner and External Release Sponsor to implement effective filtering, including an examination of timing relative to program milestones and deficiencies that could be re-used for comparable future external releases. And use this information to support the production of, if needed, a corrective POAM by the System Owner.

(3) Incorporate into the NDRB Decision Record or NDRB Administrative Record conditions that specify how the System Owner and External Release Sponsor can or cannot reuse the filtering solution developed for the NDRB evaluation for future external releases.

Appendix G. Sensitive External Release

1. APPLICATION.

a. The procedures prescribed by this Appendix apply to external releases of NAS data that meet the following criteria: the released NAS data is intended to contain sensitive NAS data, including SFD or other types of SUI/CUI; and the released NAS data is sourced by an FAA information system.

b. The procedures below are specific to Sensitive External Release and complement the procedures articulated in Chapter 3 of this order, which are common to all categories of external release.

2. TAILORED TRIGGERS FOR FULL AND TARGETED NDRB EVALUATIONS.

In addition to the basic criteria and characteristics for NDRB evaluations cited by Chapter 3, paragraphs 2 and 3 of this order, the NDRB Secretariat will use the tailored triggers indicated below to initiate Full and Targeted NDRB evaluations for Sensitive External Release cases.

a. Full NDRB Evaluation. Evaluations of this type will be initiated if one or more of the criteria listed below are met in a manner that implicates a Sensitive External Release and affects the source information system or the release itself:

(1) A novel external release of sensitive NAS data is proposed, which includes characteristics not covered by an existing NDRB Decision Record – e.g., new External Recipient, data set, proposed use case, and/or data protections.

NOTES –

1. *Reflecting the potential security ramifications of this category of external release, the NDRB Secretariat will be biased to conducting Full NDRB Evaluations for proposed releases of sensitive NAS data not thoroughly covered by a pre-existing NDRB Decision Record.*

2. *Full NDRB Evaluation will be applied as a default to requests by External Release Sponsors and/or prospective External Recipients requesting access to real-time or near real-time unfiltered NAS surveillance data to be used for testing or operations of Ground Based Surveillance System (GBSS) services facilitating Unmanned Aircraft System (UAS) integration, including Beyond Visual Line of Sight (BVLOS) operations.*

(2) A major system release or automation update is proposed for an FAA information system sourcing a Sensitive External Release, which is approved by an existing NDRB Decision Record; and potentially impacts the data protections required by that previous NDRB approval.

(3) Reported spillage of SUI/CUI by an FAA information system containing sensitive NAS data, including SFD, NAS STI, and ATO CAVI, which does not involve a Sensitive External Release approved by an existing NDRB Decision Record.

(4) Reported spillage of SUI/CUI by an FAA information system or an External Recipient, which involves a Sensitive External Release approved by an existing NDRB Decision Record.

NOTE –
Reported spillage incidents from any source will be reported to the FAA SOC

b. Targeted NDRB Evaluation. Evaluations of this type will be initiated if the following are met in a manner that implicates a Sensitive External Release and affects the source information system or the release itself. The System Owner or External Release Sponsor propose a change to an external release previously approved by the NDRB, which is not expected to materially change the data protections and other requirements established by the NDRB Decision Record and Agreements between the FAA and the External Recipient; and the source information system has submitted a System Authorization Briefing (SAB) to the ATO CRB and the change has been determined to not be a significant or substantial change.

3. TAILORED NDRB EVALUATION PROCEDURES.

In addition to the common NDRB procedures cited by Chapter 3 of this order, the NDRB Secretariat will ensure the following procedures specific to Sensitive External Release cases are implemented.

a. Pre-Coordination. The NDRB Secretariat must cooperate with the System Owner, External Release Sponsor, SFD Security Program Manager (when SFD is involved), ATO Cybersecurity Group (ACG) for all ATO SUI/CUI, and, as needed, the External Recipient, to carry out the following pre-coordination tasks before the NDRB evaluation is started:

(1) Analyze the source information system to determine what SUI/CUI, including SFD and NAS STI, is present and what SUI/CUI is to be externally released.

(2) Ensure that all External Recipients have obtained an FAA External Release Sponsor.

(3) Ensure the External Release Sponsor and External Recipient understand and are willing to comply with the information security requirements cited in Appendix H of this document as a prerequisite to the data release.

(4) Obtain *Preliminary NAS Data External Release Interagency Security Risk Statements* from the NDRB Ad Hoc Interagency Evaluators.

NOTE –
See Appendix I for an overview of the Preliminary and Final OPSEC Statements' purpose and content requirements.

(5) Ensure the External Release Sponsor and External Recipient are willing and able to develop and establish a legal agreement between the External Recipient and the FAA governing the major aspects of the proposed external release.

(6) Confirm the External Recipient's willingness and ability to secure explicit support for the proposed release of sensitive NAS data from one or more State D/As.

NOTE –
The State D/A(s) must be willing and able to protect the SUI/CUI data provided by the FAA to the External Recipient from disclosure to third parties in response to State laws and regulations promoting open records and information transparency and from other actions detrimental to the Federal Government's ability to assert FOIA

exemptions. Release by the FAA of SUI/CUI to External Recipients does not constitute a public release of information for purposes of the FOIA, 5 U.S.C. § 552.

(7) Confirm the External Recipient is a wholly U.S.-owned enterprise (or owned by a Permanent U.S. Resident), and that all affiliates associated with the proposed release, inclusive of but not limited to contractors, sub-contractors, advisors, and other partners, are also wholly U.S.-owned enterprises.

(8) If the External Recipient requests an exception to 7) above, each excepted person must, at a minimum, meet all of the following criteria to be approved by the FAA:

(a) Legal residency in the U.S., including possession of a valid green card;

(b) Minimum residency in the U.S. of at least three years within the last five years;

(c) Not be a citizen of any country identified as a U.S. adversary by the Secretary of Commerce pursuant to 15 U.S.C. § 7.4, Determination of Foreign Adversaries;

(d) Be specifically approved by the FAA as personnel essential to the activities associated with the external release use case.

(9) Confirm the External Release Sponsor and/or External Recipient are willing and able to fund costs incurred by the proposed release, including:

(a) Information security-related costs such as charges for security vetting of External Recipient personnel authorized to access the released sensitive NAS data; and

(b) Telecommunications and related network costs associated with the establishment of the external data connection, inclusive of preliminary connectivity testing.

NOTE-
Public Trust background investigations will only be scheduled after NDRB review is complete, the ATO AO has rendered a favorable authorization and risk acceptance decision, and the applicable legally binding agreements are signed. Public Trust background investigations must result in a determination of interim suitability for each person before they are allowed to access the NAS data containing SUI. If the request is disapproved by the ATO AO, no Public Trust background investigations will be conducted.

(10) Ensure any required coordination with the NAS CCB, ATO CRB, and TIS ARB is completed as prescribed by the provided procedures in Chapter 3, Section 8.

(11) Develop an NDRB evaluation plan specific to the case being discussed, including timelines and milestones; requirements for the submission of documents and other artifacts; and required actions to be completed by the System Owner, External Release Sponsor, and the External Recipient.

b. Evaluation. The NDRB Secretariat and NDRB evaluators must cooperate with the System Owner, External Release Sponsor, and External Recipient to carry out the following tasks as part of the NDRB evaluation planned during pre-coordination:

(1) **Validate Need-to-Know.** SUI and CUI are subject to dissemination controls based on "need-to-know." In this context, the External Recipient's use of the externally released sensitive NAS data must warrant the FAA's dissemination in accordance with criteria prescribed by the FAA. The External Release Sponsor, with support from the External Recipient, must present a use case for NDRB approval, which meets one or more of the following criteria:

(a) Is supported by a completed SRM analysis that confirms the proposed external release of sensitive NAS data, commonly including unfiltered NAS surveillance data, will meaningfully benefit the NAS; or

(b) Is supported by a documented analysis that confirms the proposed release of sensitive NAS data, commonly including unfiltered NAS surveillance data, is essential to an ANS or aviation regulatory function for which the FAA is responsible; or

(c) Enables testing and other exploratory activities designed to: support an SRM-based assessment of the safety benefits to the NAS provided by the proposed release of sensitive NAS data; or support some other structured assessment of benefits to an ANS or aviation regulatory function for which the FAA is responsible.

NOTE –
The NDRB Secretariat will consult specifically with AXF on the validity of the need-to-know asserted by the External Release Sponsor. AXF is the OPR for FAA Order 1600.75 and the agency's policy on protection of SUI and CUI, as part of the NDRB evaluation process.

(2) **Assess Ability to Protect.** The External Recipient must comply with the information security requirements in Appendix H to confirm their ability to protect the SUI/CUI. The NDRB will assess the External Recipient's ability to meet the requirements in Appendix H based on criteria and milestones cited in that Appendix.

(3) **Validate Duty-to-Protect.** SUI and CUI are subject to dissemination controls based on "duty-to-protect." In this context, the External Recipient must commit to the protection of the externally released sensitive NAS data in a manner that is explicitly documented by a legally binding agreement. The External Recipient, with support from the External Release Sponsor, must present a proposed legal Agreement between the External Recipient and the FAA for NDRB review, which includes the provisions listed below, along with the information security requirements cited in Appendix H. In most instances, ACG will provide the initial draft of the governing ISA, which will include the Appendix H information security requirements; changes to the ACG-provided ISA requirements can only be accomplished via coordination with the ATO AO and/or AODR. This Agreement (or set of Agreements) must be finalized and signed by FAA and External Recipient before the NDRB approves the external release through an NDRB Decision Record. The External Recipient must provide:

(a) Description of use case consistent with the asserted need-to-know presented to the NDRB;

(b) Explicit commitment to duty-to-protect;

(c) Reimbursement mechanisms by which the FAA can recover costs associated with the external release from the External Recipient, including charges related to the production, processing, and transport of the sensitive NAS data, and to required personnel security vetting.

REFERENCE –
See the following for fundamental guidance on dissemination controls for SUI and CUI related to need-to-know and duty-to-protect: 10 U.S.C. 130e, Treatment Under Freedom of Information Act of Certain Critical Infrastructure Security Information*; Executive Order (EO) 13556,* Controlled Unclassified Information*; 32 CFR 2002,* Controlled Unclassified Information (CUI)*; 49 CFR 1520,* Sensitive Security Information*; FAA Order 1600.75,* Protecting Sensitive Unclassified Information (SUI)*; FAA Order 1370.121B,* FAA Information Security and Privacy: Policy.

(4) **Information Security Compliance.** SUI and CUI are subject to extensive information security requirements, including those focused on the handling of CUI in nonfederal systems. The NDRB Secretariat will, in accordance with the procedures cited in Appendix H, disseminate the ACG-developed information security requirements package specific to the proposed external release to the External Release Sponsor and prospective External Recipient. The NDRB Secretariat, with input from the NDRB evaluators, may approve the proposed external release only when compliance with these information security requirements has been assessed and validated.

(5) **Interagency Coordination.** The NDRB Secretariat will cooperate with the participating NDRB Ad Hoc Interagency Evaluators to:

(a) Obtain expert interagency input on OPSEC and other security risks to inform the data protections to be imposed by the FAA;

(b) Obtain *Final NAS Data External Release Interagency Security Risk Statements* from the participating NDRB Ad Hoc Interagency Evaluators.

(6) **Coordination for ATO AO Authorization.** Once the NDRB evaluation has been completed, if the NDRB Chair wants to pursue an approval for the proposed release, the NDRB Secretariat will provide the completed NDRB evaluator write-ups, inclusive of concurrence and/or non-concurrence, along with the Draft NDRB Decision Record and draft legal agreements, to ACG for action, in accordance with the procedures cited in Appendix H of this document.

(7) **NDRB Authorization and Follow-Up.**

(a) The NDRB will restrict external releases in the NDRB Decision Record based on use cases for which need-to-know still needs to be validated, to the duration and other minimum parameters needed to enable testing and other exploratory activities intended to support the validation of the proposed use case through the FAA's SRM process or other structured assessment addressing benefits to an ANS or aviation regulatory function for which the FAA is responsible.

(b) The NDRB Secretariat will incorporate into the NDRB Decision Record: expectations for sustained compliance with the data protections (including SCM and MoSR provisions) required by the FAA; and non-compliance triggers for FAA action to withdraw external release approval and terminate access to released sensitive NAS data.

Appendix H. Information Security Requirements

1. APPLICATION.

a. The procedures below support NDRB evaluations of Sensitive External Release cases in accordance with Appendix G. This appendix guides the NDRB Secretariat's cooperation with the NDRB Evaluators to formulate and confirm the implementation of the FAA's information security requirements prior to approving the external release of sensitive NAS data, specifically including NAS STI and SFD qualified as SUI/CUI, in accordance with Federal Government policies and standards for handling CUI in non-federal systems.

b. The NDRB Secretariat may use the procedures below to inform coordination with other FAA offices regarding the sharing of NAS data wholly among FAA information systems and work on NDRB Evaluations for Sustained External Release (see Appendix E) and Focused External Release (See Appendix F) cases.

2. PREREQUISITE REQUIREMENTS TO BE ELIGIBLE FOR NDRB CONSIDERATION.

The NDRB Secretariat will work with the External Release Sponsor for each potential External Recipient to ensure that the minimum prerequisites are fully met prior to coordination with ACG on the applicable Security Control Measures (SCM) requirements for the proposed release. In addition to those requirements cited in Appendix G, section 3.b, the External Requestor must:

a. Limit all NAS data processing, storage, and offline storage to physical locations in the U.S., inclusive of any cloud processing and storage.

b. Limit access to the NAS data containing SUI/CUI to only those personnel, inclusive of the requestor's personnel, contractors (and sub-contractors), advisors, and other partners, who are sole U.S. citizens or otherwise specifically approved by the FAA.

c. Limit the use of any Artificial Intelligence (AI) software and/or hardware to AI specifically approved by the ATO AO.

3. SECURITY CONTROL MEASURES (SCM).

a. Once the NDRB Secretariat has ensured that prerequisites in Appendix G and section 2 above are fully met, the Secretariat and the External Release Sponsor must initiate coordination with ACG to request the applicable information security requirements, referred to as SCMs in this order, for the proposed release.

NOTE-
ACG will follow FAA information security policy and applicable NIST standards, generally NIST SP 800-171 and NIST SP 800-171A, to formulate the SCMs, which will consist of approximately 150 specific requirements. At its discretion, ACG may consult with the NDRB Secretariat, other NDRB evaluators and/or other FAA offices in the requirements development phase

b. The NDRB Secretariat will provide the ACG-developed SCM requirements package to

the External Requestor.

c. The External Requestor must fully implement all of the SCM requirements into all systems intended to process, transmit, store, or provide access to the FAA SUI/CUI.

d. The External Requestor's system boundary, infrastructure, data flows, and security controls must be implemented, baselined, documented, and able to be assessed for the system intended to contain NAS SUI/CUI.

e. The External Requestor must complete an ACG-approved Third-Party Assessment Organization (3PAO) security assessment of their level of compliance with each of the requirements and/or controls in the SCM requirements package.

f. Prior to the request undergoing NDRB review, all required outputs of the 3PAO security assessment must be analyzed by ACG, and a preliminary risk assessment, inclusive of any stipulations and/or other conditions to be placed on the External Requestor, must be signed by the ATO AODR and provided to the NDRB Secretariat.

NOTE –
Timelines for the ACG analysis will vary based on workload but will generally require a minimum of 60 business days.

g. The NDRB Secretariat must ensure that all stipulations and/or conditions provided by the ATO AODR are incorporated into the draft legally binding agreements prior to NDRB review.

h. The NDRB Secretariat must include the written ATO AODR preliminary risk assessment documentation in the evaluation package for NDRB review.

4. NDRB-SPECIFIC REQUIREMENTS.

a. The External Recipient must designate and maintain a primary and backup System Security Officer (SSO). These SSOs are responsible for ensuring the External Recipient's compliance with all SCM requirements imposed by the FAA and maintaining coordination with the FAA on sustained compliance matters such as personnel vetting, spillage, and other security incidents.

b. The External Recipient must designate and maintain a primary and backup System Security Officer (SSO). These SSOs are responsible for ensuring the External Recipient's compliance with all SCM requirements imposed by the FAA and maintaining coordination with the FAA on sustained compliance matters such as personnel vetting, spillage, and other security incidents.

c. The External Recipient must limit retention of NAS SUI/CUI to what is minimally needed to support the use case supporting the external release authorized by the NDRB.

d. The External Recipient must agree to and fully implement a means approved by the FAA to prohibit "down streaming" the released NAS SUI/CUI to any entity that is not specifically approved by the FAA, subject to the requirements of the legal Agreement governing the external

release between the External Recipient and the FAA, and legally obligated to comply with the SCM and MoSR provisions imposed by the FAA.

NOTES –

1. This prohibition of down streaming by External Recipients specifically applies to further disseminating SFD used by the External Recipient to provide GBSS and other services enabling BVLOS to subscribing UAS operators and other third-parties, including other UAS service suppliers.

2. FAA approval of any foreign national key personnel is contingent on the ability of the FAA to conduct the personnel screening for the proposed foreign national

e. External Recipient personnel requiring access to the sensitive NAS data released by the FAA, at the discretion of the FAA in cooperation with interagency security partners, may be required to undergo successful vetting prior to being approved by the FAA to access sensitive NAS data containing SFD or other SUI/CUI.

5. MITIGATION OF SENSITIVITY RISKS (MOSR).

a. The NDRB Secretariat and NDRB evaluators will cooperate with the External Release Sponsor and as needed, System Owner and External Recipient to formulate and require the implementation of a MoSR package tailored to individual Sensitive External Release cases.

b. MoSR provisions are intended to mitigate the OPSEC and other security consequences of unauthorized access to sensitive NAS data released by the FAA externally, specifically focusing on external releases of SFD containing SUI/CUI, despite the required SCM requirements.

c. MoSRs are executed by the FAA and are typically applied to the sensitive NAS data prior to transport outside of the FAA network to the External Recipient's systems.

d. The NDRB will typically require multiple MoSR provisions to be applied, including the typical requirements listed below:

(1) Redact, remove, or otherwise withhold one or more data elements from the NAS data feed to be externally released, which may enable third parties to identify the government D/A operating sensitive flights or the individual flight(s).

NOTE –
External releases of NAS radar data are likely to be sourced prior to ingestion by FAA ATC automation systems such as ERAM and STARS, which means that correlated flight plan data, such as Aircraft Identification (ACID), are intentionally not included.

(2) Limit the NAS surveillance data to that which is minimally needed to meet the use case-based needs of the External Recipient.

(3) Tailor the service volume of the provided NAS surveillance data to meet the minimum use case-based needs of the External Recipient through geographic and altitude-based limitations.

(4) Release data that has select elements redacted, removed, or otherwise withheld from

the provided feed.

(5) Prohibit any unnecessary sharing of radar site characterization data, including radio frequencies; transmit power; emission characteristics (e.g., bandwidth and modulation, as well as pulse width and repetition rate); antenna setup (e.g., gain, polarization, height above ground); and measured radius of coverage at all altitudes.

(6) Obfuscate one or more data elements from the NAS radar data feed.

6. FINAL ATO AO AUTHORIZATION AND NDRB APPROVAL.

a. When the NDRB evaluation is complete, in instances where the NDRB Chair wants to pursue an approval for the proposed release, the NDRB Secretariat will provide the completed NDRB evaluator write-ups, inclusive of concurrence and/or non-concurrence, along with the draft NDRB Decision Record, to the ACG NDRB Evaluator(s) for review and authorization by the ATO AO.

NOTE –
The NDRB Secretariat will coordinate a timeline with ACG to obtain the ATO AO response, generally 30 business days at a maximum.

b. ACG will prepare a recommendation for the ATO AO based on the ability of the External Recipient to adequately protect NAS SUI/CUI as required.

c. The ATO AO will render a written decision for the proposed release indicating either authorization for the connection and for the release of the NAS SUI/CUI, including any additional stipulations and/or conditions; or a non-concur.

d. In instances where the ATO AO accepts the risk for the proposed release and authorizes the connection and the release of NAS SUI/CUI, the NDRB Chair may move forward with NDRB approval.

e. In instances where the ATO AO does not accept the risk for the proposed release, a written non-concur will be provided at either the AO and/or the AODR signature level, and the NDRB Chair must disapprove the proposed release.

Appendix I. NDRB Evaluation Process Documentation Requirements

1. PURPOSE.

a. This appendix provides information on documentation requirements that the System Owner or the External Release Sponsor will be responsible for coordinating and providing to the NDRB Secretariat to support an NDRB evaluation.

b. While this appendix describes a broad list of documents and information that may be required, each NDRB evaluation situation has unique attributes. The NDRB Secretariat will tailor the specific documentation requirements with the FAA System Owner or the FAA Sponsor during the NDRB evaluation *pre-coordination phase* cited in Appendices E, F, and G.

2. NDRB EVALUATION PACKAGE DOCUMENTATION REQUIREMENTS.

a. Process. The NDRB Secretariat will collaborate with the System Owners and External Release Sponsors to tailor the specific information required to execute an NDRB evaluation based on the details of each NDRB evaluation request and derived from this and other FAA orders, current NDRB SOP guidance, and any other applicable references. While the following is intended to provide a general overview of the presentation and documentation requirements, the NDRB Secretariat will provide more specific information.

b. Presentation requirements. All NAS data release requests will require the FAA System Owner or the External Release Sponsor to collaborate with the NDRB Secretariat to develop and schedule a presentation in Microsoft PowerPoint format, which provides specific details regarding the request. The presentation should include: system diagrams, identification of SUI/CU data elements, deployment schedules, and other details derived from the documentation requirements listed in paragraph c below. The System Owner or External Release Sponsor will use the presentation to brief the NDRB Secretariat, NDRB evaluators, and NDRB Chair on the particulars of individual external release cases.

c. Documentation requirements. System Owners and/or External Release Sponsors must collaborate with the NDRB Secretariat to submit specific documentation, as applicable, from the following list. This list may not be all-inclusive or apply in every instance, depending on the specific system characteristics or external request use case, but generally includes:

(1) Completed FAA Form 1200-5, *NAS Data Release Request*. See Appendix D.

(2) Messaging Service and Web Service Description Documents.

(3) TIS ARB documented FNTB testing results.

(4) System Security Plans, characterization documents, architecture/overview diagrams, SUI/CUI data elements and security, connections, data marking/tagging/filtering, current users, any included proprietary data, etc.

(5) Current legally binding agreements with external entities receiving SUI/CUI.

(6) Status of compliance with any previous NDRB Decision Records and update on any SUI/CUI spillage mitigation plans.

(7) Artifacts characterizing implementation of or compliance with FAA-mandated SCM and MoSR provisions, as well as relevant requirements of FAA Orders 1600.75 and 1370.121.

(8) Implementation/deployment milestones status and timelines (e.g., key site dates).

(9) Any other documentation requirements specifically required by and listed in Appendix E, F, or G not cited above.

d. Interagency Input on Security Risks. The following statements are required from each NDRB Ad Hoc Interagency Evaluator participating in an NDRB evaluation of a Sensitive External release case

(1) **Preliminary NAS Data External Release Interagency Security Risk Statements**. This statement must address any concerns with the external non-Federal entity's operational environment prior to scoping the SCM, MoSR legal agreements, and other data protection requirements. This is intended to provide an initial assessment of potential OPSEC risks to public aircraft operations based on the external requestor's proposed system characterization and concept of operations (CONOPS) and by the proposed NAS data release if no protective actions were taken.

(2) **Final NAS Data External Release Interagency Security Risk Statements**. The final statement must take into consideration the proposed risk mitigations, including SCMs and MoSRs outlined in legally binding agreements levied as a condition of the sensitive NAS data release. See Appendix H for details. This is intended to document specific SCMs, MoSRs, CONOPS, or other changes implemented that reduced the perceived OPSEC risk and document any perceived "residual" OPSEC risks following the system's demonstration of compliance with the legal agreement requirements.

3. NDRB DECISION RECORD.

a. The NDRB Secretariat will ensure NDRB Decision Records clearly state what is approved for external release and identify any conditions associated with the approval or disapproval of the release. NDRB release approvals vary depending on the sensitivity of the NAS data.

b. Typical NDRB Decision Record approved actions include, but are not limited to, the following:

(1) An external release system can be approved to release non-sensitive near real-time and/or historical NAS data from the identified release and/or version of that system to any external entity, including the public, via the external connection(s) specified in their NDRB Decision Record (if applicable). Non-sensitive NAS data can be articulated in various ways, inclusive of but not limited to the specific language below:

(a) Filtered NAS data (all SFD removed) as confirmed by AJR-2 and AXF-200.

(b) Redacted NAS data (all NAS STI and/or ATO CAVI redacted, removed, or otherwise withheld) as confirmed by AXF-200 and ACG.

(c) Sanitized NAS data (substantially modified NAS data that no longer contains SUI/CUI, as confirmed by AXF-200).

(d) Inherently non-sensitive NAS data, such as non-proprietary weather data, as confirmed by AXF-200.

(2) An FAA information system can be approved by the NDRB to release non-sensitive historical data, as confirmed by AXF-200, only from their system to any External Recipient. See above for descriptions of non-sensitive NAS data.

(3) An external release system can be approved to continue releasing sensitive NAS data to existing External Recipients that have been revalidated by the NDRB.

(4) FAA users of external release systems or optional evaluation systems that do not contain sensitive NAS data can be approved to share any NAS data from that system with external entities.

(5) FAA users of information systems containing SFD, which are engineered to allow the user the ability to extract filtered NAS data (all SFD removed) from that system, may be approved by the NDRB to share filtered NAS data from that system with external entities, provided it does not contain SFD, NAS STI, or ATO CAVI.

(6) An External Recipient can be approved to receive sensitive NAS data for a specified time period and a specified use or purpose.

c. NDRB Decision Records approving data release must include the following “conditions of release”, at a minimum:

(1) Requirement for full compliance with all stipulated data protection measures and authorization from ATO AO.

(2) Prohibition on further downstream sharing of any sensitive NAS data to any entity or individual not specifically included in the Decision Record.

(3) A data retention limitation of 45 days unless otherwise included in the Decision Record.

(4) FAA requirement that any suspected or known spillage or unauthorized disclosure of the FAA-provided SUI/CUI is reported. Include a reporting time constraint and FAA point of contact based on the specific NAS data release situation.

(5) For requests made for sensitive NAS data for test purposes, a clear description of all

test data that the External Recipient needs to provide the FAA to support validating their use case, inclusive of the FAA office that needs to evaluate the data, POC contact information, and method of transmitting the test data to the FAA. If no test data criteria are provided, include a statement indicating as such.

(6) Sensitive NAS data must not be transmitted to the External Recipient until there is an NDRB Decision Record signed by the NDRB Chair approving the release of the sensitive NAS data to that specific External Recipient.

d. NDRB Disapproval with Conditions and/or Recommendations. NDRB Decision Record Disapproval is possible for, but not limited to, the following situations:

(1) Failure to meet need-to-know requirements.

(2) Failure to meet duty-to-protect data protection requirements.

(3) Failure to properly implement SFD filtering requirements or failure to receive SFD filtering validation from AJR-2.

e. Failure of existing or proposed connections to meet information security requirements. Duration of the NDRB Decision Record. The NDRB Decision record remains in effect unless the occurrence of one of the events cited in Chapter 3 of this order. NDRB Decision Records approving sensitive NAS data release for testing are limited to one (1) year from provisioning of the date.