

**BY THE ORDER OF THE COMMANDER
NORTH AMERICAN AEROSPACE
DEFENSE COMMAND (NORAD) AND
UNITED STATES NORTHERN COMMAND
(USNORTHCOM)**

**NORAD AND USNORTHCOM
INSTRUCTION 33-194 VOLUME 6**



20 SEPTEMBER 2013

Communications and Information

**HEADQUARTERS NORAD AND
USNORTHCOM INFORMATION
GOVERNANCE VOLUME 6 - PORTAL
PROGRAM**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: NORAD and USNORTHCOM publications and forms are available on the NORAD and USNORTHCOM portal page for downloading <https://portal.noradnorthcom.mil/library/Pubs/SitePages/Home.aspx>

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: N-NC/CSKM

Certified by: N-NC/CSD (Col Ronald L. Banks)

NNCI33-188, 25 January 2013

Pages: 31

This instruction prescribes NORAD and USNORTHCOM policies and procedures for establishing and maintaining the NORAD and USNORTHCOM Portal. This instruction applies to all personnel within NORAD, USNORTHCOM and subordinate units. It is meant to supplement, not override, any direction from the Chairman, Joint Chiefs of Staff (CJCS), Service Department, or Department of Defense Agency directives. It does not apply to Air Force Reserve Command or National Guard units. This instruction may not be supplemented. Send recommendations to change, add, or delete information in this instruction to HQ NORAD and USNORTHCOM, ATTN: N-NC/CSKM, 250 S. Vandenberg Street, Suite B016, Peterson AFB, CO 80914-3020 using AF Form 847, *Recommendation for Change of Publication*. Maintain and dispose of records created as a result of prescribed processes in accordance with the Joint Staff Disposition Schedule CJCSM 5760.01A, *Joint Staff and Combatant Command Records Management Manual: Vol I (Procedures) and Volume II (Disposition Schedule)*. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the U.S. Government. See **Attachment 1** for a list of references and supporting information.

1. Purpose/Objective	2
2. Applicability/Audience	3
3. NORAD and USNORTHCOM Portal Vision	3
4. NORAD and USNORTHCOM Portal Guiding Principles	3
5. Roles and Responsibilities	4
6. Procedures	6

7. Releasability	7
8. Scope	7
9. Risks	7
10. Location	7
11. Waivers	7
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION	8
Attachment 2—PERMISSIONS MANAGEMENT	9
Attachment 3—GOVERNANCE HIERARCHY	12
Attachment 4—APPLICATION USAGE POLICIES	16
Attachment 5—TRAINING	29
Attachment 6—SUPPORT PLAN	30

1. Purpose/Objective. The objective of this instruction is to establish governance strategy, methods, and policies for usage and management of the NORAD and USNORTHCOM Portal(s).

1.1. This document outlines the administration, maintenance, and support of NORAD and USNORTHCOM's Portal environments. It identifies lines of ownership for operational, business and technical teams. It also defines who is responsible for what areas of the system. It ensures the system is managed and used in accordance with its designed intent to prevent it from becoming unmanageable.

1.1.1. The management of this enterprise Portal system involves both a strategic, business-minded board to craft rules and procedures for its use, and also a tactical, technically-competent team to manage the routine operational tasks that keep the system running. Users of the system are empowered to improve and recommend changes through the change management process (see **Attachment 3**).

1.2. Additional objectives:

1.2.1. Identify appropriate organization representatives to provide insight and direction for the Portal, and the ability to implement these initiatives within their respective organizations.

1.2.2. Create an effective support system with proper channels of escalation for end users of the Portal environments.

1.2.3. Communicate the need for NORAD and USNORTHCOM leaders to provide support to the system in the form of trained, technically talented users able to customize, personalize, and use the Portal in a manner that employs capabilities identified by the Knowledge Management Board (KMB).

1.2.4. Enforce this policy as appropriate, and evaluate and adjust policy, as necessary, over the life cycle of the system.

1.2.5. Create and enforce a standardized process to manage portal access for all users external to NORAD and USNORTHCOM.

2. Applicability/Audience. This document is intended to be read by all members of the KMB and all key users of the Portal environment (administrators, Site Collection Owners (SCO), Site Owners (SO), customizers, and portal community). General Portal users are also encouraged to be familiar with this document.

2.1. Key users defined:

2.1.1. Portal Administrators. Select personnel from Chief of Staff, Knowledge Management (N-NC/CSKM) Office and N-NC/J67 who are trained in Portal administration and development. These individuals will receive "SharePoint Farm Administration" permissions across all Portals.

2.1.2. Site Collection Owners. Director approved/selected individuals who have completed SCO training and are assigned to a specific site collection. Each site collection will have one primary and one alternate person assigned. These individuals will have "Full Control" permissions, to include content organizer development (minus site creation) across all sites within their collection. SCOs will be required to have Active Directory Users and Computers installed on both NIPR and SIPR computers in order to manage their security groups. SCOs approve and select individuals to be Site Owners (see below).

2.1.3. Site Owners. Individuals who have completed SO training and are assigned to a specific site. Each site will have one primary and one alternate person assigned. These individuals will have "Full Control" permissions (minus site creation and permission management) of their site.

2.1.4. Customizer. N-NC/CSKM approved individuals who have received and completed specialized training using SharePoint Designer 2010 by a certified vendor. The number of people with this permission will be extremely limited due to the damage one can cause by improperly using the program. Requests for the software will have to be approved by the N-NC/CSKM office before the Service Desk will install it on an individual's computer. Individuals who have not completed training in SharePoint Designer will not have it loaded on their workstation(s).

2.1.5. Portal Community. Individuals within each organization that are interested in how the Portal can be improved and are willing to attend frequent meetings to discuss issues/improvements with N-NC/CSKM and SCOs. There is no limit to the numbers of personnel in the portal community.

3. NORAD and USNORTHCOM Portal Vision. A secure, customizable, browser-independent thin client, globally available to NORAD and USNORTHCOM personnel, components, subordinates, regions, and sectors, as well as our mission partners. The Portal uses open standards to expose innovative services tailored to support the NORAD and USNORTHCOM missions and enhance information sharing and collaboration.

4. NORAD and USNORTHCOM Portal Guiding Principles:

- 4.1. Provide a modern Portal with improved collaboration capability.
- 4.2. Provide the ability to share information with appropriate safeguards.
- 4.3. Provide the ability to use Active Directory (AD) to improve security management.
- 4.4. Enable SCOs/SOs to manage access to their data in directorate or office collections.

- 4.5. Provide simple access to functional collections to enable collaboration with mission partners and other external organizations.
- 4.6. Provide community capabilities.
- 4.7. Provide the ability to personalize content and My Sites based on user roles.
- 4.8. Improve command processes.
- 4.9. Incorporate records management into the Portal.

5. Roles and Responsibilities:

5.1. N-NC/CSKM:

- 5.1.1. Portal promotion.
- 5.1.2. Create and maintain user training strategy.
- 5.1.3. Function as focal point for user feedback and enhancement.
- 5.1.4. Secretariat for requirements submission to KMB.
- 5.1.5. Prepare training materials customized for NORAD and USNORTHCOM based on leadership guidance and customer feedback.
- 5.1.6. Train and support users throughout the implementation of the new Portal, as well as, post implementation. Develop and conduct stand-alone and refresher training for end users and advanced users.
- 5.1.7. Enforce site standards (layouts, security processes, etc.).
- 5.1.8. Conduct provisioning of all sites and sub-sites.
- 5.1.9. Portal development:
 - 5.1.9.1. Provide architectural guidance.
 - 5.1.9.2. In conjunction with the N-NC/J6, develop infrastructure and operation best practices. Build the framework and features of the Portal.
 - 5.1.9.3. Maintain visual design for a consistent “look and feel” across the entire portal.
 - 5.1.9.4. Modify templates as needed.
 - 5.1.9.5. Provide desk side or telephonic assistance upon request for any non-technical issues.
- 5.1.10. SharePoint application:
 - 5.1.10.1. Build new Web Parts and write ASP.NET code.
 - 5.1.10.2. Build and maintain applications or web parts that leverage Key Performance Indicator (KPI) data Business Intelligence (BI), reporting, dashboards, and data analytics with the assistance of business analysts.
 - 5.1.10.3. Communicate with the staff to gather requirements.
- 5.1.11. Maintain and update Portal taxonomy and governance.

- 5.1.12. Provide final approval for external account requests (Joint Task Force Trusted Information Exchange (JTFTIE) and Secure Joint Task Force Trusted Information Exchange (SJFTIE)) portal access after validation by the NORAD and USNORTHCOM sponsor.
- 5.1.13. Create and enforce records management policies and Records Bucket taxonomy.
- 5.1.14. Provide content strategy (type, frequency, refreshing, and expiration).
- 5.1.15. Provide Tier 3 support as necessary.
- 5.2. N-NC/J6:
 - 5.2.1. Provide Tier 1, 2, and 3 support to users (refer issues to Tier 4 [vendor personnel] when necessary), see **Attachment 6**.
 - 5.2.2. Provide SharePoint server and operating system patches and updates.
 - 5.2.3. Ensure network and infrastructure connectivity, security, and maintenance.
 - 5.2.4. Conduct user account management (e.g. SharePoint user accounts/AD account management).
 - 5.2.5. Responsible for SharePoint database, site collection, and site backups for local SharePoint server.
 - 5.2.6. Responsible for global Portal configuration, shared services, policies, and procedures.
 - 5.2.7. Manage Portal security.
 - 5.2.8. Ensure continuity of operations and disaster recovery support for Portal.
- 5.3. Organizational leadership:
 - 5.3.1. Select and appoint personnel to SCO and SO positions.
 - 5.3.1.1. An appointment letter is required for SCO positions and is optional for SO positions. The appointment letter template can be found on the Portal (located under Communities > Portal Communities). These are kept on file in the N-NC/CSKM Office.
 - 5.3.2. Ensure content is being managed properly.
- 5.4. Site Collection Owner/Site Owner:
 - 5.4.1. Administer and maintain sites under their purview.
 - 5.4.2. Manage security for all sub-sites, pages, document libraries, and Lists under their purview.
 - 5.4.3. Maintain content and ensure relevancy.
 - 5.4.4. Assist N-NC/CSKM on content strategy (type, frequency, refreshing and expiration).
 - 5.4.5. Content approval when necessary.
 - 5.4.6. Manage the site layout (visual design) and structure.
 - 5.4.7. Attend and complete required SCO/SO training.
 - 5.4.8. Represent the organization at "Portal Community" meetings.
 - 5.4.9. Populate and manage AD security groups for assigned sites.

5.4.10. Ensure completeness and accuracy of all Requests for Change (RFC) submitted from within respective organization. Submit RFCs as outlined in **paragraphs A3.2. – A3.2.5.**

5.5. Users:

5.5.1. Create and maintain content where user has Contributor permissions.

5.5.2. Attend all required user training.

5.6. NORAD and USNORTHCOM KMB:

5.6.1. Seek out opportunities for improvement and enhancement of system capability.

5.6.1.1. Approve Portal strategy within the commands.

5.6.1.2. Approve changes to the Portal Governance policy.

5.6.1.3. Provide direction and guidance to the N-NC/CSKM on leveraging the Portal to increase the efficiency and collaborative capabilities within the commands.

5.6.1.4. Approve significant structural or design changes to the Portal.

5.6.1.5. Create and/or drive possible synergies that can be developed among organizations and divisions using the Portal environment.

5.6.1.6. Coordinate with groups/agencies that are undertaking similar initiatives to understand how other organizations share associated knowledge, processes, and technologies to their mutual advantage.

5.7. Portal Advisory Working Group (PAWG):

5.7.1. Comprised of representatives from across the commands with expert knowledge in their subject area.

5.7.2. Provide recommendations on change packages to the KMB.

5.7.3. Review proposed packages and provide a recommendation of “Approve” or “Reject” based on findings.

5.8. NORAD and USNORTHCOM Sponsor. A US military or government civilian employee assigned to NORAD and/or USNORTHCOM, a Component Command, NORAD Region, or Subordinate Command who has knowledge of a person from an outside organization that is requesting access to the NORAD and USNORTHCOM portal, and agrees that the applicant has an operational need for access.

5.9. External User. A person external to NORAD and USNORTHCOM who is a mission partner, or has an operational need to access the portal(s). The external user must have a NORAD and/or USNORTHCOM sponsor in order to request access. External users requesting access who do not have a NORAD and/or USNORTHCOM sponsor will be denied access. External users must register for a JTFTIE and/or SJTFTIE account for access to the NIPRnet and SIPRnet portals respectively. Initial access to the portal(s) by an external user will be restricted to the common collaborative areas of the portals (Home, Events, Functions, Communities, Libraries, and MSC/CDCF). Additional access will be requested through each site and approved by the site owner or site collection owner.

6. Procedures. See Attachments 2 through 6:

6.1. **Attachment 2:** Permissions Management

- 6.2. **Attachment 3:** Governance Hierarchy
- 6.3. **Attachment 4:** Application Usage Policies
- 6.4. **Attachment 5:** Training
- 6.5. **Attachment 6:** Support Plan

7. Releasability. Unclassified.

8. Scope. This Governance manual includes NORAD and USNORTHCOM Portal environments including development, staging and production.

9. Risks. The following are risks to an effective governance strategy:

- 9.1. Inadequate support from within the organization to affect proper governance.
- 9.2. Administrators or users refusing to abide by the given policies in this directive.
- 9.3. Lack of policy enforcement.

10. Location. This directive will be posted in the Portal library section of each Portal.

11. Waivers. Waivers or deviations from this directive are at the discretion of the Chief of Staff. Substantial justification for non-compliance with the Governance Change Process, described in **Attachment 3**, must exist before a waiver request will be considered.

CHARLES D. LUCKEY, Major General, USA
Chief of Staff

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION**

Amendment to Section 508, Federal Rehabilitation Act, 13 July 2000

44 U.S.C., Chapter 44, *Disposal of Records*, 3 January 2012

CJCSI 5760.01A, *Records Management Policy for the Joint Staff and Combatant Commands*, 30 April 2007, Current 18 July 2012

CJCSM 5760.01A Vol I, *Joint Staff and Combatant Command Records Management Manual: Volume I -- Procedures*, 7 February 2008, Ch2, 13 July 2009

CJCSM 5760.01A Vol II, *Joint Staff and Combatant Command Records Management Manual: Volume II-- Disposition Schedule*, 13 July 2012

DODD 5400.11, *DOD Privacy Program*, 8 May 2007, Ch1, 28 July 2011

DODD 8320.02, *Data Sharing in a Net-Centric Department of Defense*, 2 December 2004

DODM 5200.01 V2, *DOD Information Security Program Marking of Classified Information*, 24 February 2012, Ch1, 31 March 2012

CJCSM 3213.02C, *The Joint Staff Focal Point (FP) Program*, 31 March 2009

NNCHOI 90-123, *Records Management*, 1 April 2005

(b)(2)



Figure A2.1. (b)(2)

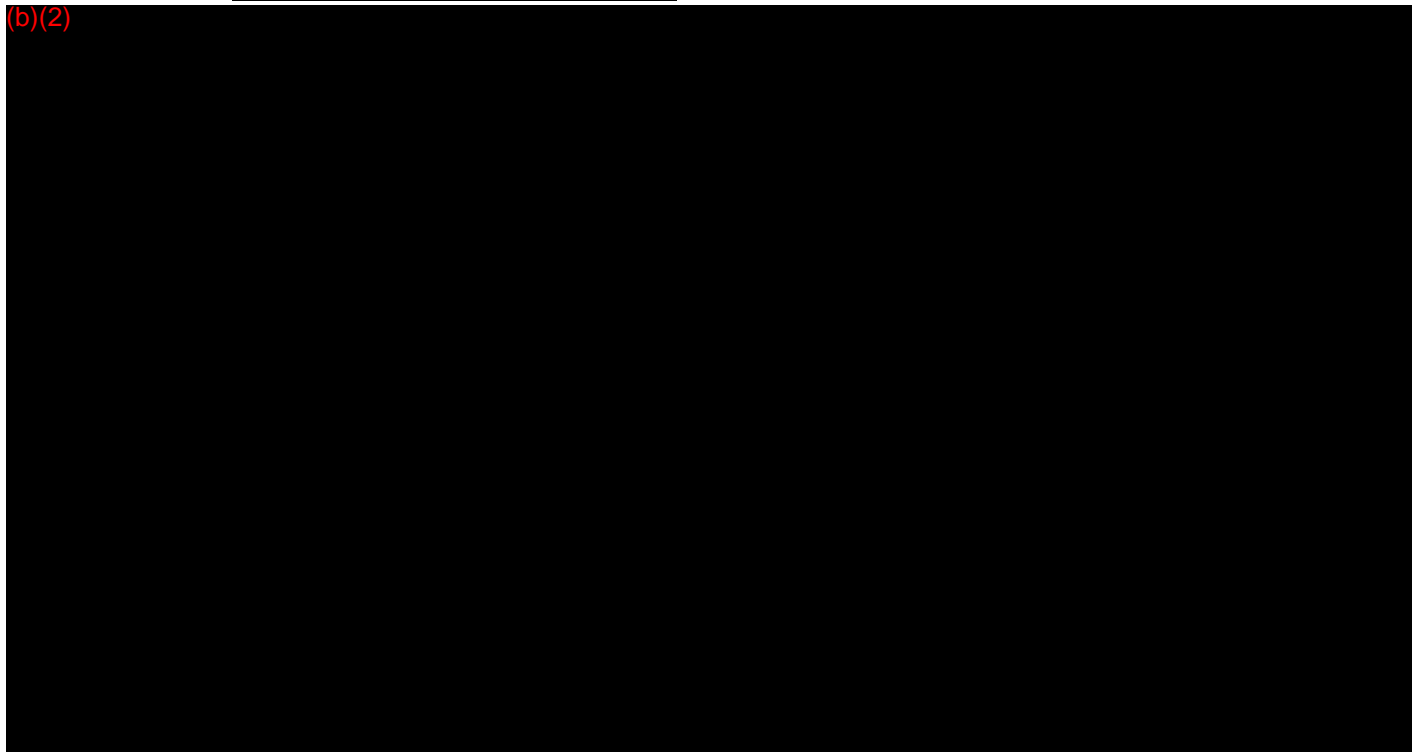


Figure A2.2. (b)(2)

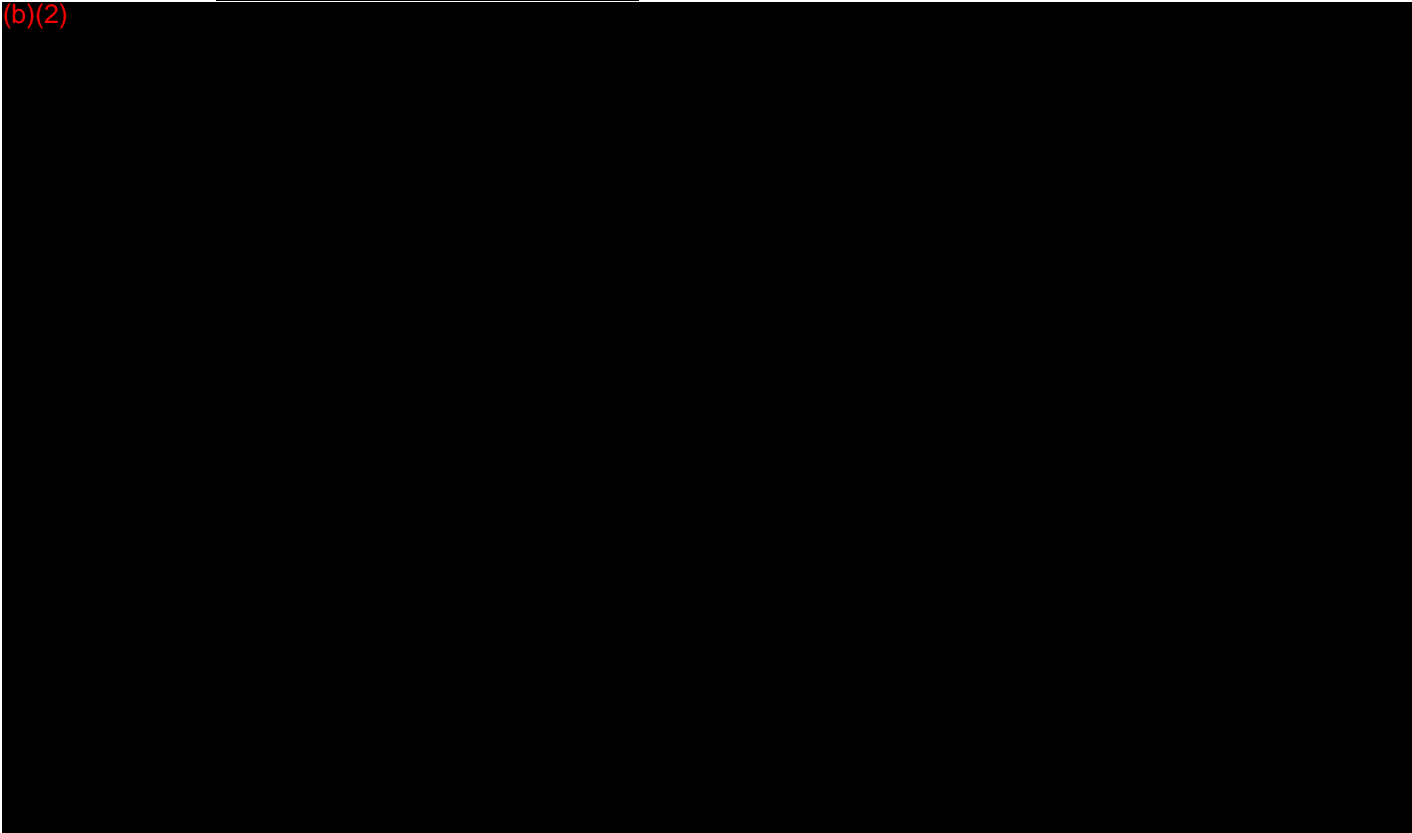
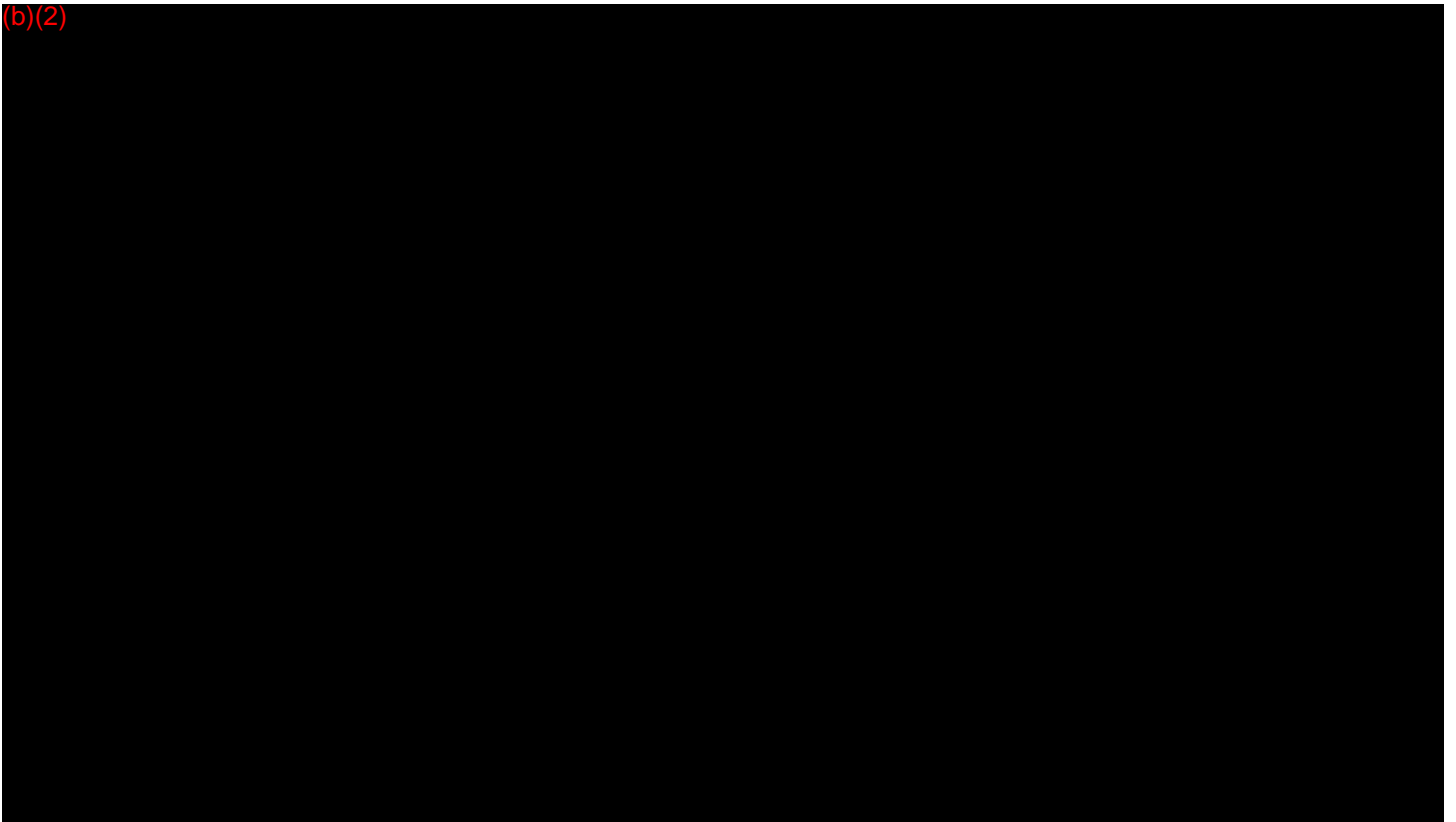


Figure A2.3. (b)(2) [Redacted]



Attachment 3

GOVERNANCE HIERARCHY

A3.1. Governance. The Portal Governance process will provide a unified, centrally governed approach for changes to the Portal environments. The KMB is the overriding authority for decisions, including architecture, design, development support, and governance policies. It serves as the arbiter between customer requests and the developer/technical manager. The KMB strongly influences foundational and framework-related issues.

A3.1.1. KMB. This board consists of designated staff representatives who provide strategic insight and direction for the Portal and who are able to drive strategic initiatives within their respective organizations. The KMB will review packages from the PAWG and make an overall recommendation for the N-NC/CS. The N-NC/CS will make the final decision on what action is taken. The KMB will consist of, at a minimum (additional members at the discretion of the N-NC/CS):

- A3.1.1.1. Chairperson – N-NC/CS
- A3.1.1.2. N-NC/Deputy Chief of Staff of Knowledge Management (DCSKM)
- A3.1.1.3. N-NC/J1
- A3.1.1.4. N-NC/J2
- A3.1.1.5. N/J3
- A3.1.1.6. NC/J3
- A3.1.1.7. N-NC/J4
- A3.1.1.8. N-NC/J5
- A3.1.1.9. N-NC/J6
- A3.1.1.10. N-NC/J7
- A3.1.1.11. N-NC/J8
- A3.1.1.12. N-NC/J9
- A3.1.1.13. N-NC/S&T

A3.1.2. Portal Advisory Working Group. This working group provides recommendations on change packages to the KMB and is comprised of representatives from across the commands with expert knowledge in their subject area. The working group will collectively decide whether or not the package should be given an “Approve” or “Reject” recommendation. The working group will consist of individuals from the following offices (additional members at the discretion of the N-NC/DCSKM):

- A3.1.2.1. Chairperson – N-NC/DCSKM
- A3.1.2.2. Information Assurance
- A3.1.2.3. OPSEC
- A3.1.2.4. Architecture
- A3.1.2.5. Knowledge Management
- A3.1.2.6. Portal Management

- A3.1.2.7. FOIA/PA
- A3.1.2.8. Foreign Disclosure
- A3.1.2.9. Records Management
- A3.1.2.10. Historian
- A3.1.2.11. Resource Manager
- A3.1.2.12. Information Management

A3.1.3. Portal Community Group. This group meets regularly to discuss issues within the Portal environment, and for users to make recommendations for potential modifications. N-NC/CSKM will facilitate these meetings and ensure each request for change is thoroughly discussed. The user presenting the request will complete the Portal Change Request Form (found on the Portal under Communities > Portal Communities) and provide it to N-NC/CSKM for submission to the PAWG (see **Figure A3.1**). During the meeting(s), N-NC/CSKM will provide additional training to the users on new features within the Portal or other requested training. The Portal Community Group will consist of individuals from the following groups, at a minimum (additional members at the discretion of the N-NC/CSKM):

- A3.1.3.1. N-NC/CSKM
- A3.1.3.2. SCO
- A3.1.3.3. Representative from each Directorate (may also be the SCO)
- A3.1.3.4. Users with a desire to improve the Portal

A3.2. Portal RFC Process: **Figure A3.2**. Shows the process for changes to this Portal governance or to the physical or logical structure of the Portal. The following steps will be taken by each group within the process and escalated to the next level if it exceeds the threshold for approval at their level.

A3.2.1. User Community: Users within the Commands who use the Portal and identify issues that need to be fixed/added/changed and submit the request to the SCO or SO in their directorate who will bring it to next Portal Community Group meeting in the form of a completed RFC form (see **Figure A3.1**).

A3.2.2. Portal Community Group: The Portal Community Group will review each RFC and decide if it is allowed by the current governance directive. If so, the Portal Community Group may approve the change and assist the user in implementing the change. If the RFC would violate the governance, or require changes to the architecture, it must be forwarded to the PAWG for review. SCOs and/or SOs are responsible for ensuring RFCs are accurate, complete and submitted to N-NC/CSKM. The Portal Community Group will meet monthly, unless changes in Portal operation require more frequent meetings.


A3.2.3. Portal Advisory Working Group: The SCO/SO who champions the RFC will brief the PAWG and answer any question they may have. Following each RFC brief, the PAWG will vote on said RFC. Members of the PAWG will vote “approved” or “disapproved.” Disposition of the RFC is based on a majority vote of the PAWG. For RFCs that must be referred to the KMB for decision, they will move forward with a recommendation from the PAWG to approve or disapprove the RFC. RFCs that are deferred will be sent back to the submitting SCO/SO for more information or scheduled for a later meeting of the PAWG. If the RFC does not require funding or

changes to the governance directive, the PAWG may approve it at their level without forwarding it to the KMB. The PAWG will meet every other month or as directed by the N-NC/CSKM.

A3.2.4. KMB: Each RFC will be briefed to the KMB by the SCO/SO who submitted the RFC and answer any questions of the board. Following all RFC briefs, the KMB will discuss each RFC and vote to “approve,” “disapprove,” or “defer” the RFC. RFCs that are deferred will be sent back to the submitting SCO/SO for more information or scheduled for a later meeting of the KMB. The KMB will meet at least once a quarter, unless current situations require a quicker decision on an RFC. Meeting more frequently will be at the discretion of the N-NC/CS. Approved RFCs will be forwarded to N-NC/CSKM and N-NC/J67 for implementation.

A3.2.5. RFC History: N-NC/CSKM will be responsible for maintaining a record of all RFCs that go through the process which includes the dates each RFC met each level of the process and the outcome. This list will be made available on the Portal for all users to review so similar requests are not submitted in the future.

Figure A3.1. Portal Request for Change (RFC) Form.




NORAD and USNORTHCOM Portal Request For Change (RFC)

Summary Information

Title


Description


Justification for Change

Submitter 

Details

Site URL (if applicable)

Site Collection Owner 

Site Owner 

Estimated cost to Government

Approval Coordination





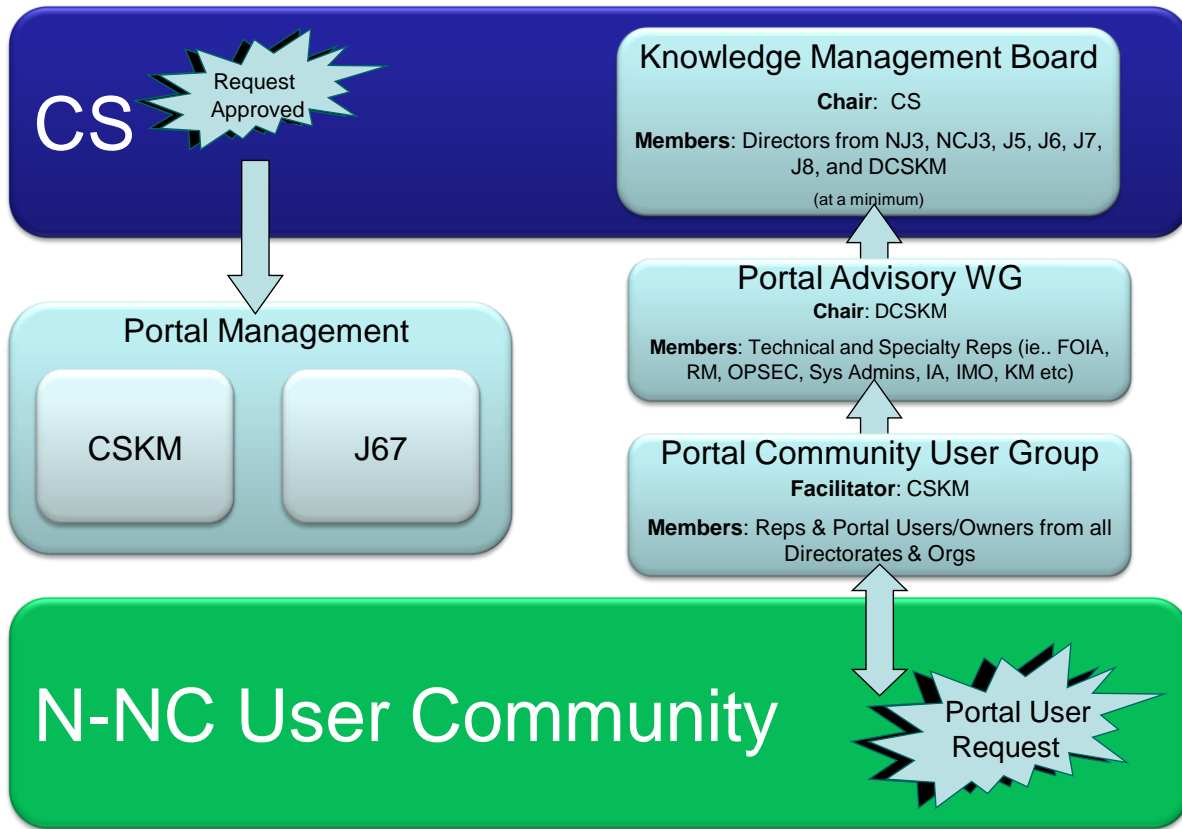
Super Users Group	<input style="width: 95%;" type="text"/>		Status	<input style="width: 95%;" type="text" value="Select..."/>	Date	<input style="width: 95%;" type="text"/>
Portal Advisory WG	<input style="width: 95%;" type="text"/>		Status	<input style="width: 95%;" type="text" value="Select..."/>	Date	<input style="width: 95%;" type="text"/>
KM Board	<input style="width: 95%;" type="text"/>		Status	<input style="width: 95%;" type="text" value="Select..."/>	Date	<input style="width: 95%;" type="text"/>
N-NC/CS	<input style="width: 95%;" type="text"/>		Status	<input style="width: 95%;" type="text" value="Select..."/>	Date	<input style="width: 95%;" type="text"/>

Figure A3.2. Portal Change Hierarchy.

Portal Governance Hierarchy



Attachment 4

APPLICATION USAGE POLICIES

A4.1. General Guidelines. The Portal is a tool used by NORAD and USNORTHCOM, Component Commands, Subordinate Commands and other external users for collaboration, notification, and analysis information supporting operations in the NORAD and USNORTHCOM Area of Responsibility (AOR).

A4.1.1. Portal information is current, relevant, and usable information related to ongoing operations or collaboration efforts. The Portal is intended to be a collaborative platform for sharing information among NORAD and USNORTHCOM sub-organizations and, if needed, other agencies regarding current events within NORAD and USNORTHCOM's AOR.

A4.1.1.1. All material will be handled in accordance with its specific disposition rules set out by the organization's approved File Plan.

A4.1.2. Information must be organized in a defined, structured manner.

A4.1.3. Information must conform to a defined management lifecycle to reduce duplication, and to keep Portal information current, relevant, and usable. It must also meet Federal legal requirements for preservation and disposition. In general, information should be handled in accordance with records management procedures as outlined in NNCHOI 90-123, *Records Management*.

A4.1.4. Information should be maintained in only one location. If information is needed for reference by a different group of users, a link to the information should be created on a site to point users to the appropriate location or document. This saves storage resources and ensures the most up-to-date information is available.

A4.1.5. Users should use Links, Announcements, Really Simple Syndication (RSS) feeds, and other inherent SharePoint capabilities on their respective site to avoid cluttering organization sites with unnecessary information and to reduce reliance on e-mail as a means of collaboration or information dissemination. Documents that originate from sources outside the Portal should not be saved on the Portal if at all possible. These documents should be referenced with links to ensure users are accessing the most current version from the originating source.

A4.1.6. Users may set alerts by selecting the "Alert Me" option, or using RSS, on document and list libraries, which they frequent in order to stay abreast of changing and emerging information while still minimizing excess distribution of document copies and reducing the use of limited storage space to hold redundant and reference information.

A4.1.7. Site auto expiration. To ensure stale sites are removed and data storage is reclaimed, sites untouched for 90 days may be slated for deletion/archival. SOs will be notified if their site is slated for deletion/archival and will be provided with a mechanism to remove it from the list. Before any content is deleted or archived, SCOs/SOs and organizational Records Officers will coordinate with Command Records Manager to ensure proper retention and disposition are applied.

A4.1.8. SCOs, SOs and Customizers must complete required training and pass a skills assessment, if required, prior to obtaining elevated permissions on Portal sites.

A4.1.9. Storage Quotas:

A4.1.9.1. SCOs shall receive alerts when storage is at 90 percent of quota. The standard allocation for storage for each Site Collection is managed by N-NC/CSKM and N-NC/J67, depending on the organization and the amount of initial data.

A4.1.9.2. SharePoint Administrators can override storage quota for Site Collections only upon approval of N-NC/DCSKM and consideration with N-NC/J67 on available physical storage. If unsure of the impact of a change, the request must go through the Governance Change process described in **Attachment 3**.

A4.2. Organization Main Pages:

A4.2.1. The main page of an organization’s site is intended to be the location that users external to the organization can visit for information about current activities and key information. It is not intended to be a working location for draft documentation or collaboration efforts. In essence, the organization main page(s) represent the “pulse” of the organization, where users can readily identify key personnel, events, products and a map of available information.

A4.2.2. At a minimum, organizations are required to have certain items on their directorate and division level sites as listed in **Table A4.1**. below. The template used to create sites will contain most items and it is the responsibility of the SO to add/remove web parts as necessary to comply with **Table A4.1**.

Table A4.1. Required and Optional Items.

Required on Directorate/Division Page	Optional on Directorate/Division Page
Director/Division Chief Photo	Organization Chart
Director/Division Chief Bio Link	Announcements
Director/Division Chief Sig block	Libraries
Mission/Vision	Lists
SCO Name(s) and Contact Information	Logos/Images
SO Name(s) and Contact Information	Key Leadership Contact List

A4.2.3. SCO/SO point of contact (POC) information will be displayed on each Portal site.

A4.2.4. Page lengths should be limited so that the information contained on the page does not exceed the height of the page on a standard 3:4 monitor display. This is to try and prevent users from having to scroll down to find information.

A4.2.5. Page widths should be limited so that the information contained on the page does not exceed the width of the page on a standard 3:4 monitor display. This is to try and prevent users from having to scroll right to find information.

A4.3. Other Pages:

A4.3.1. My Sites. Each user on the Portal will have a My Site with a storage limit of 100MB. The My Site is designed to store documents and data that are used by that user and may be viewed by other users on the Portal. Profile information is limited to professional information only. The My Site storage limits do not allow the site to be used as a collaboration site and users should plan

on collaborating on documents on other sites within the Portal. Users will ensure their profile information is up to date and the following fields are filled in (**Table A4.2.**): Note that some of the optional information is Personally Identifiable Information and should be protected as such.

Table A4.2. My Site Requirements.

Required My Site Profile Information
Office Location
Past Projects - Specify all N-NC Program names
Skills - Specify all skills to include Technical skills, Language proficiencies, Military skills (F-22 Pilot, Infantry, etc...), and anything else that may be utilized within N-NC
Optional My Site Profile Information
Picture
Mobile Phone
FAX
Home Phone
Time Zone (May be changed to match your location)
Assistant
Schools
Birthday

A4.3.2. Conference Sites. All conferences hosted by NORAD and USNORTHCOM (even if they are being held at NORAD and USNORTHCOM) will be requested using the online Conference Request Form located in the “Action Officers Toolbox” under “Conferences.” Approval will result in the creation of a conference site and addition to the list of upcoming conferences. Each conference site will be managed by a SO from the requesting directorate/special staff. All conference sites will be opened up to all Portal users with contributor permissions so they may register for the event. The SO may restrict specific libraries to registered users by coordinating with N-NC/CSKM. Following the conference, each site will be archived into the Records Repository for read-only access.

A4.3.3. Organizational/Unit Sites. Organizational/Unit Sites are designed for use by the organization/unit only. Members of each organization/unit will be part of the Contributors on their respective organization/unit’s site. All other members of NORAD and USNORTHCOM will have read only permission on all other organization/unit sites main pages unless mission requirements require further restrictions. Each unit (subordinate or component command) will have similar permissions established to allow unit members the ability to contribute and other unit members to read. Members of one command will not be given read permission to subordinate sites within another command.

A4.3.4. Functional and Community sites: Sites within these site collections will be made open to all users as readers, unless mission requirements dictate further restrictions. Users requiring contribute permissions will request access at each site through SharePoint Access Request controls.

The primary supported organization for functional and community sites will be the SCO for their sites respectively. In conjunction with the SCO, N-NC/CSKM will determine SOs for these sites.

A4.4. Site Design:

A4.4.1. The use of SharePoint Designer on the NORAD and USNORTHCOM Portal will be restricted in order to maintain a standard visual design across all pages and prevent the accidental deletion of data large sections of the Portal. The use of SharePoint Designer will be restricted at each site collection by disabling page detachment, master page customization, and management of the web site URL structure (See **Figure A4.1.**). Remaining permissions will allow Customizers to develop workflows, connect to external data sources, and make modest modifications to pages. The use of SharePoint Designer will be unrestricted for Site Collection Administrators (N-NC/CSKM Portal Personnel) across each web application.

Figure A4.1. SharePoint Designer Settings.

<p>Allow Site Owners and Designers to use SharePoint Designer in this Site Collection</p> <p>Specify whether to allow Site Owners and Designers to edit the sites in this Site Collection using SharePoint Designer. Site Collection Administrators will always be able to edit sites.</p>	<p><input checked="" type="checkbox"/> Enable SharePoint Designer</p>
<p>Allow Site Owners and Designers to Detach Pages from the Site Definition</p> <p>Specify whether to allow Site Owners and Designers to detach pages from the original Site Definition using SharePoint Designer. Site Collection Administrators will always be able to perform this operation.</p>	<p><input type="checkbox"/> Enable Detaching Pages from the Site Definition</p>
<p>Allow Site Owners and Designers to Customize Master Pages and Page Layouts</p> <p>Specify whether to allow Site Owners and Designers to customize Master Pages and Page Layouts using SharePoint Designer. Site Collection Administrators will always be able to perform this operation.</p>	<p><input type="checkbox"/> Enable Customizing Master Pages and Page Layouts</p>
<p>Allow Site Owners and Designers to See the Hidden URL structure of their Web Site</p> <p>Specify whether to allow Site Owners and Designers to view and manage the hidden URL structure of their Web site using SharePoint Designer. Site Collection Administrators will always be able to perform this operation.</p>	<p><input type="checkbox"/> Enable Managing of the Web Site URL Structure</p>

A4.4.2. Sites and pages shall remain consistent in appearance with the NORAD and USNORTHCOM main Portal page. This applies to all pages on all NORAD and USNORTHCOM Portals. Changes to the visual design must be approved by the Governance process before implementation

A4.4.3. Organization personnel will not use web page editing tools, such as SharePoint Designer, to modify the site template or master pages. Pages will only be modified with the SharePoint browser interface to minimize the number of customized NORAD and USNORTHCOM Portal sites. SharePoint Designer capabilities will be limited, and distribution will be allowed on a case-by-case basis to those individuals who have completed SharePoint Designer training by a certified vendor and approved by N-NC/CSKM. Organization-level master pages and page templates should be closely managed, particularly for common information types (mission, POCs, calendars, department links, etc). However, organizations should also be able to post information unique to their mission that may require custom templates and master pages created by a Customizer.

A4.4.4. Sites will be created with established, standardized site templates and will not be modified from those templates except when approved by the Governance process. By default, N-NC/CSKM should utilize the NORAD and USNORTHCOM standard templates when creating a Portal Site. Initial template load will include templates for Organizational sites, Conference Sites, Functional Sites and DSCA events. Any requests for new templates, and/or master pages, or changes to existing templates and/or master pages will be made via a Site Request Form and validated by N-NC/CSKM (See **Figure A4.2.**). N-NC/CSKM will create the approved template and ensure it is made available across all applicable site collections.

Figure A4.2. Site Request Form.

The screenshot shows a web form titled "NORAD and USNORTHCOM Request for Portal Site". At the top left are two logos: the NORAD logo and the USNORTHCOM logo. The form is organized into sections with grey headers:

- Summary Information:** Contains four input fields: "Title", "Description and Special Instructions", "Reason for Site (And why it cannot be done with a page)", and "Submitter".
- Individual Details:** Contains three input fields: "Site URL Requested", "Site Collection Owner", and "Site Owner".
- Security Groups Required:** Contains one input field: "Name of Security Group". Below this field is a checkbox labeled "Insert item".

A4.4.5. As a guideline, sub sites should be no more than three levels deep from any top level site. A site should contain no more than 40 libraries (Document or List). An organization page should display no more than 20 web parts, if web parts remain collapsed on the page, or 10 web parts if any web parts are expanded on the page. These suggestions are intended to ensure minimal load times on Portal sites, particularly for remote users or users in low-bandwidth environments. If a site requires a large amount of resources, consideration should be given to splitting the site up into additional sites.

A4.5. Security:

A4.5.1. Guidelines for marking unclassified (e.g. U//FOUO) documents, extending to classified information will be adhered to, including portion marks, and declassification instructions IAW DODM 5200.01 V2, *DOD Information Security Program Marking of Classified Information*. Classified information will only be posted to the SIPR Portal.

A4.5.2. All sites and sub-sites will have a master page security banner clearly reflecting the highest classification and caveat.

A4.5.3. Documents must be marked properly, tagged with their classification level, and stored in a Portal approved for information up to and including the documents' classification.

A4.6. Document Libraries, Lists, and Information Lifecycle Management:

A4.6.1. Folder use within document libraries will be minimized due to the limited navigability of libraries containing folders. Folders should not be more than two levels deep within a document library.

A4.6.2. No more than 500 documents will be maintained in each individual document library. This restriction is intended to ensure manageability of content and rapid page load times, particularly for users in areas with low bandwidth.

A4.6.3. Each list or library on the Portal must contain a description that accurately describes its function.

A4.6.4. No more than 10,000 list items will be maintained in each list library. If list libraries contain attachments, they should be treated with the same restrictions as document libraries. This restriction is intended to ensure manageability of content and rapid page load times.

A4.6.5. In order to define and apply disposition, a required "Record Bucket" metadata field will be applied to all Portal Libraries and applicable lists. See **Figure A4.3.** for example. SCOs will coordinate with organization SOs before creating new Libraries or Lists to ensure proper Record Bucket options are available and Content Organizer rules can be created. NOTE: The Portal will be integrated with the Records Repository, called HP TRIM.

A4.6.5.1. Record Buckets. In order to ensure records management compliance, appropriate metadata must be assigned to all files on the Portal. Categories for assigning metadata to files are derived from the approved file plan provided by each organization's Records Officer.

A4.6.6. If a document is created in the course of Command business, it is a record and it must be tagged with a Record Bucket option. If a record is not a Command business product and is, therefore, a reference, it must be tagged with a Reference option.

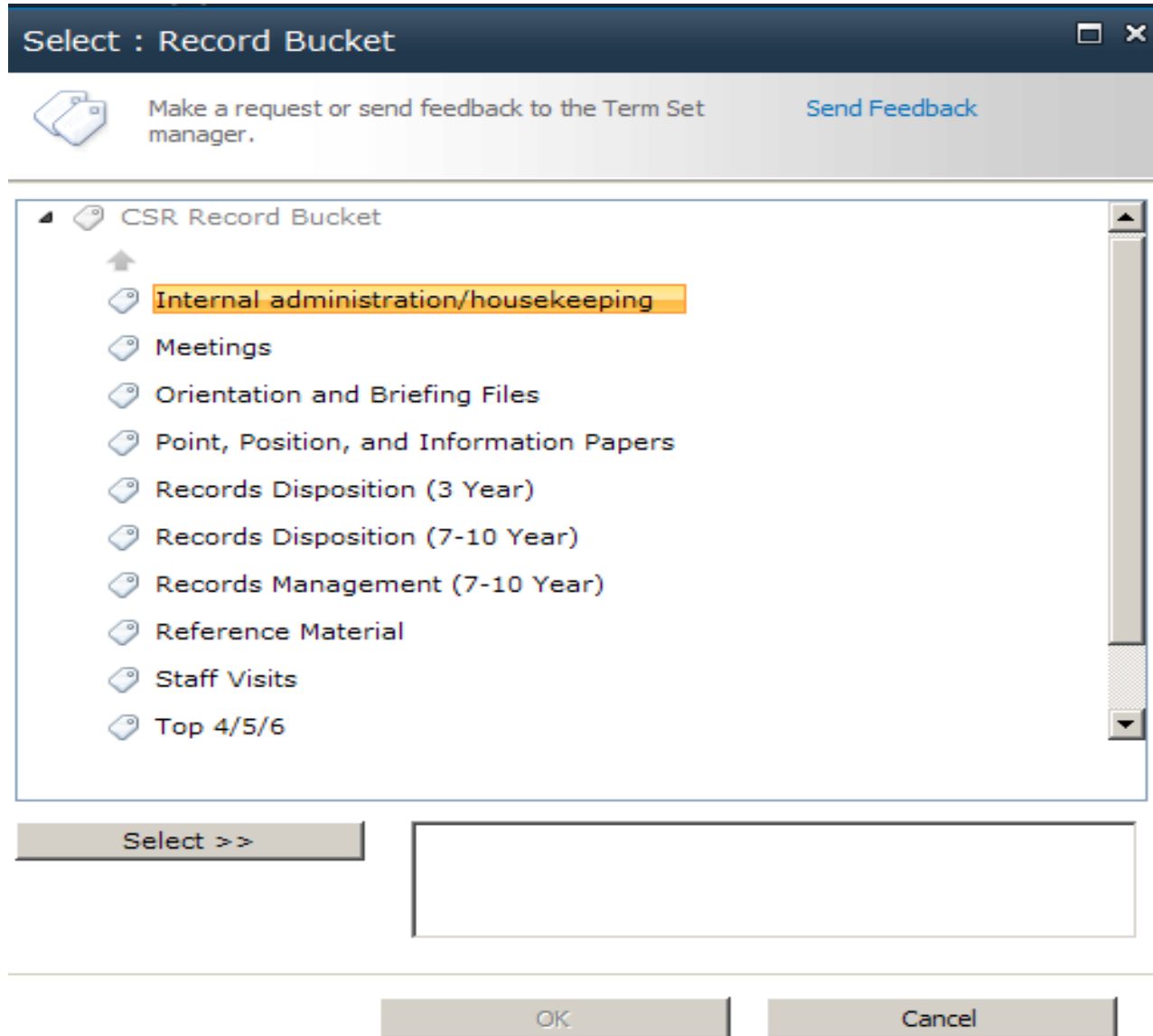
A4.6.7. If document versioning is enabled for a library, SOs must ensure that no more than 10 versions shall be saved to the repository.

A4.6.8. 508 Compliance: Individuals with permissions higher than "Contributor" anywhere on the Portal will try to ensure sites are in compliance with Section 508 of the Federal Rehabilitation Act. Since the Portal is an internal facing Portal, there will be no requirement to do so. Individuals with Customizer permissions will use the Compliance Checker feature of SharePoint Designer 2010 to ensure sites are as close to compliant as operationally possible.

A4.6.9. Personally Identifiable Information (PII): Information that can identify an individual outside of NORAD and USNORTHCOM can be stored in document libraries on the

Portal. SOs will ensure that sites with PII are only accessible by those who need access to them for official use. Examples of this are organization social rosters, anything containing a Social Security Number, etc. SOs with questions about PII should contact the N-NC/CSKM office for further guidance/education.

Figure A4.3. Record Bucket.



A4.7. Web Parts:

A4.7.1. Only Web Parts validated by the KMB and approved and installed by N-NC/CSKM will be used on the NORAD and USNORTHCOM production Portal. No outside or third party web parts will be used without authorization from N-NC/CSKM and the KMB. Users who require additional web parts will submit an RFC requesting a web part be added. This requirement will be validated and approved through the governance process and N-NC/J67 Change Management process. The KMB may recommend a commensurate capability in lieu of the requested web part, in order to further standardize Portal capabilities across NORAD and USNORTHCOM.

A4.7.2. A web part library shall be maintained for approved web parts to maximize reuse.

A4.7.3. The addition of scripts/code to a site is prohibited, unless approved by Information Assurance. All approved scripts/code will be maintained in a global code library where it may be used by others as necessary. N-NC/CSKM will maintain this global library on the Portal and ensure any file submitted to the library is approved by Information Assurance.

A4.8. SharePoint Groups and Permissions. This section will discuss the default SharePoint groups, authorized custom SharePoint groups, the commensurate permission levels authorized, group ownership guidance, and the restrictions on membership and employment of those groups.

(b)(2)

A4.8.1. Site Owners Security Group:

A4.8.1.1. (b)(2)

SCOs will be responsible for informing N-NC/CSKM when members depart or change roles.

A4.8.1.2. SCOs and SOs responsible for managing the site will be included in this group. A minimum of two qualified organization personnel (or other N-NC/J6 personnel, if applicable) must be included in this group. Staff elements should limit membership to the lowest number absolutely required after the first two are identified and trained, and ensure that at least one is a government employee. Transfer of Portal roles shall be incorporated into out-processing checklists.

A4.8.1.3. No personnel will be granted membership to a SOs group until they have reviewed this policy, and have received appropriate N-NC/CSKM approved Portal training.

A4.8.1.4. (b)(2)

A4.8.1.5. (b)(2)

A4.8.2. Group Ownership:

A4.8.2.1. (b)(2)

A4.8.2.2. (b)(2)

A4.8.3. Customizers:

A4.8.3.1. (b)(2)

A4.8.3.2. (b)(2)

A4.8.3.3. (b)(2) [Redacted]

A4.8.3.4. No personnel will be granted membership to a customizers group until they have reviewed this policy and have received appropriate Portal training.

A4.8.4. Members:

A4.8.4.1. (b)(2) [Redacted]

A4.8.4.2. (b)(2) [Redacted]

A4.8.4.3. (b)(2) [Redacted]

A4.8.5. Visitors:

A4.8.5.1. (b)(2) [Redacted]

A4.8.5.2. (b)(2) [Redacted]

A4.8.5.3. (b)(2) [Redacted]

A4.8.6. Custom Permissions Levels. Any additional custom permission levels or SharePoint groups shall be created by Site Collection Administrators only, and validated by the governance process, as required.

A4.8.7. Site Pages Document Libraries:

A4.8.7.1. (b)(2) [Redacted]

A4.8.7.1.1. (b)(2) [Redacted]

A4.8.7.1.2. (b)(2) [Redacted]

A4.9. Resource Domain Security Groups:

A4.9.1. (b)(2) [Redacted]

A4.9.1.1. (b)(2) [Redacted]

A4.9.1.2. (b)(2) [Redacted]

A4.9.1.3. (b)(2) [Redacted]

A4.9.1.4. (b)(2) [Redacted]

A4.9.1.4.1. (b)(2) [REDACTED]

A4.9.1.4.2. (b)(2) [REDACTED]

A4.9.1.4.3. (b)(2) [REDACTED]

A4.9.2. (b)(2) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

A4.9.3. (b)(2) [REDACTED]
[REDACTED]

A4.9.4. (b)(2) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

A4.9.5. (b)(2) [REDACTED]
[REDACTED] [REDACTED]
[REDACTED]
[REDACTED]

A4.9.6. (b)(2) [REDACTED]
[REDACTED]

A4.9.6.1. (b)(2) [REDACTED]

A4.9.6.2. (b)(2) [REDACTED]

A4.9.6.3. (b)(2) [REDACTED]

A4.9.6.4. (b)(2) [REDACTED]

A4.9.6.5. (b)(2) [REDACTED]

A4.9.6.6. (b)(2) [REDACTED]

A4.10. (b)(2) [REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

A4.11. Customization:

A4.11.1. Requests for customization of web parts, web sites, document libraries, list libraries, or other SharePoint components should be submitted through a RFC. User configuration of approved web parts is permitted without having to submit a RFC.

A4.11.2. Customizations possible through standard SharePoint administration tools may be accomplished by the organization SO. Customizations made through the use of SharePoint Designer may be made by individuals with Customizer permissions.

A4.11.3. Additional requests for customization for alternate tools will be requested through the RFC process.

A4.12. Custom Development. Anything that is not “Out-of-the-box” functionality is considered custom development. In order to ensure a secure and functional Portal, all customizations must follow a specific process that includes the governance process, development environments, Test and Integration Laboratory (TIL) environments, and the production Portal.

A4.12.1. All customizations deployed to the production Portal must be thoroughly tested in the NORAD and USNORTHCOM TIL. Features will be deployed to the production Portal by N-NC/J67 or N-NC/CSKM through the use of .wsp files. All .wsp files deployed to the Portal will be maintained in a secure code library where access is limited to N-NC/CSKM and N-NC/J67.

A4.12.2. The TIL will mirror the production Portal as close as possible and provide an area to thoroughly test any proposed customizations. Access to the TIL is only allowed through dedicated computers that are not on the NIPR network; it will not be accessible remotely. N-NC/CSKM members will be the Portal Administrators for the SharePoint application within the TIL. Any features requiring advanced development tools will be developed in the N-NC/CSKM Development Lab and deployed to the TIL using .wsp files.

A4.12.3. N-NC/CSKM will maintain a development laboratory which provides developers and administrators the ability to develop and test advanced features and code before introduction to the TIL. The development TIL will not be connected to the NORAD and USNORTHCOM TIL or production network. The development laboratory will have an outside connection to the “dirty internet” to facilitate development and maintenance of the network. N-NC/CSKM is responsible for operations and maintenance of the development laboratory. N-NC/CSKM will have access to a NORAD and USNORTHCOM Microsoft Developer Network license for use in the development laboratory.

A4.13. My Sites. Each user of the Portal will have access to “My Site;” an area of the portal that can be customized to the user’s preference. Users are required to maintain their profile information and may upload a photo of their face to allow others to see their image around the Portal.

A4.14. Organization of the Portal. The NIPR Portal is comprised of the following Site Collections and areas:

A4.14.1. Home – Reserved for use by N-NC/CSKM and Public Affairs. This is the first site all users will see when they go to the Portal and it will contain current information about the commands. The Master Navigation Bar will allow users to connect to other sites within the Portal.

A4.14.2. Events – Designed to house sites for events that are open to the larger audience of Portal users. Conferences, Distinguished Visitor visits, operational events, and current exercises will reside here. The default permission level for all sites will be “Reader” for all Portal users. Sites may be made more restrictive if mission requirements dictate.

A4.14.3. Functions – Contains sites for the common functions at NORAD and USNORTHCOM that are open to the larger audience of all users. The default permission level for all sites will be “Reader” for all Portal users. Sites may be made more restrictive if mission requirements dictate.

A4.14.4. Organizations – Houses sites for each of the Directorates or Special Staff at NORAD and USNORTHCOM. The intent is for permissions to be given only to those members of the organization. The default permission level for all users of a certain organization is “Contributor.” Sites may be made more restrictive if mission requirements dictate.

A4.14.5. Units - Houses sites for each of the Subordinate and Component Commands of NORAD and USNORTHCOM. The intent is for permissions to be given only to those members of the unit. The default permission level for all users of a certain organization is “Contributor.” Sites may be made more restrictive if mission requirements dictate.

A4.14.6. Communities – Designed to be used by Portal users who share a common desire to collaborate on activities not covered by the functional areas. The default level of permission for all users will be “Reader” on all sites. SOs may elevate community members to “Contribute” permissions as required. Sites may be made more restrictive if mission requirements dictate.

A4.14.7. Records Repository – The single repository for final documents of NORAD and USNORTHCOM. Final documents are those documents that are no longer made available for editing and represent official decision and/or historical documents for the commands. All Headquarters users will be given “read” access so they may search the repository for information. External Users will be given access on a case-by-case basis, as determined by the Command Records Manager and the content owner.

A4.14.8. Search – Allows users to search the entire Portal and the Records Repository for documents, lists, etc. for those items to which they have at least “read” permissions.

A4.14.9. Productivity Hub – Contains help materials for all Microsoft® Office suite tools.

A4.14.10. Synchronization Hub – Used to synchronize content type and site columns across the Portal. Access is restricted to Portal administrators.

A4.15: Classification of Portal items

A4.15.1. All libraries and lists will have a required field for classification. Default values are not allowed. The following values are available in NIPR:

A4.15.1.1. UNCLASSIFIED

A4.15.1.2. UNCLASSIFIED//FOUO

A4.15.1.3. UNCLASSIFIED//LES

A4.15.2. The following values are available in SIPR:

A4.15.2.1. UNCLASSIFIED

A4.15.2.2. UNCLASSIFIED//FOUO

A4.15.2.3. UNCLASSIFIED//LES

A4.15.2.4. CONFIDENTIAL//NOFORN

A4.15.2.5. CONFIDENTIAL//REL USA, ACGU

A4.15.2.6. CONFIDENTIAL//REL USA, CAN

A4.15.2.7. CONFIDENTIAL//REL USA, MEX

A4.15.2.8. CONFIDENTIAL//REL FVEY

A4.15.2.9. SECRET//NOFORN

A4.15.2.10. SECRET// REL USA, ACGU

A4.15.2.11. SECRET//REL USA, CAN

A4.15.2.12. SECRET//REL USA, MEX

A4.15.2.13. SECRET//REL FVEY

A4.16. Access to sensitive areas of the Portal. Portal Administrators who, by default, have access to all areas of the Portal, will be considered Trusted Agents in accordance with CJCSM 3213.02C, *The Joint Staff Focal Point (FP) Program*, GL-4. Each organization is responsible for monitoring who has access to sensitive areas of their respective portal pages.

A4.17. Master Navigation Menu. Changes to the master navigation menu will be requested through the RFC process.

A4.18. Records Management. All content created by NORAD and USNORTHCOM users belong to the organization, not the individual, and must be managed in accordance with NNCHOI 90-123. To facilitate this management, each organization will develop and submit a File Plan to be approved by the Command Records Manager. In doing so, the Command Records Management Office will add needed metadata to the Record Bucket that is available on the Portal, as illustrated below (**Figure A4.3**). By choosing the appropriate Record Bucket and sending to the Records Repository when no longer needed for operational use, the applicable disposition will be applied to correctly manage the content.

A4.19. Content may be made available to foreign nationals only with the requisite foreign disclosure authority. The Portal's posting process will help to identify the foreign disclosure authority, or lack thereof, for each item posted.

Attachment 5

TRAINING

A5.1. Training Plan:

A5.1.1. An effective training plan is required if users are going to adopt the system and use it effectively in their daily activities. Training requirements are listed below:

A5.1.1.1. All users will require Portal training. User training will be conducted monthly by N-NC/CSKM.

A5.1.1.2. SCOs and SOs need advanced training, including office integration and security policies. SCO and SO training will be conducted quarterly.

A5.1.1.3. All users need usage overview training to include security policies.

A5.1.1.4. Service Desk personnel require intense training and troubleshooting analysis. Tier 2 or Tier 3 support should be considered for official, externally-provided training.

A5.1.1.5. Training begins with elementary tasks and progresses to more difficult tasks, culminating with administrator level tasks and administrator certification.

A5.1.1.6. Training tools may include:

A5.1.1.6.1. "How to" documentation

A5.1.1.6.2. Instructor-led training

A5.1.1.6.3. Online labs hosted in an off-line environment

A5.1.1.6.4. Demonstrations during Portal Community Group meetings

A5.1.2. N-NC/J6 will provide specialized training for those with elevated Portal privileges.

Attachment 6

SUPPORT PLAN

A6.1. Support for the Portal will be provided via a multi-tiered approach. The support system consists of a network of support professionals as listed below:

A6.1.1. End User Support:

A6.1.1.1. Tier 0 support – SCOs/SOs will be the primary end user support contact for their location.

A6.1.1.2. Tier 1 Support – Service Desk.

A6.1.1.3. Tier 2 Support – Escalation to N-NC/J67 Collaboration Team/System Administrators and/or N-NC/CSKM.

A6.1.1.4. Tier 3 Support – Microsoft® vendor support.

A6.1.2. Support Availability. See **Table A6.1.** below.

Table A6.1. Support Availability.

Support Group	Special Functions	Availability
Tier 0 SCO/SO	<ul style="list-style-type: none"> ▪ Assist users to find online help ▪ Basic product support; general how to and troubleshooting ▪ Design and permissions for the organization, community or functional site ▪ Design and permissions for the organization and other owned sites ▪ Creation and assigning site ownership of sub-sites (organization, community or functional) ▪ Site access issues ▪ Change site ownership ▪ Information Management Lifecycle questions and policies ▪ Assist users to Tier 1, 2 or 3 level support 	Depends on working hours of SCO/SO personnel
Tier 1 Service Desk	<ul style="list-style-type: none"> ▪ Basic product support; general how to and troubleshooting ▪ Assists in pushing issues to next level tiers 	7 days x 24 hours
Tier 2 N-NC/CSKM Collaboration Team System Administrators	<ul style="list-style-type: none"> ▪ Create or delete Portal sites ▪ Redirect or rename site ▪ Site restore requests ▪ Increase storage quota ▪ Resolve escalated issues ▪ Off-hours site access issues 	Normal duty hours, on call 7 days x 24 hours
Tier 3 N-NC/J67	<ul style="list-style-type: none"> ▪ Addresses all issues that have been unresolved at the previous tiers 	As needed
Tier 4 Vendor	<ul style="list-style-type: none"> ▪ Addresses all issues that have been unresolved at the previous tiers 	As needed