DEPARTMENT OF THE NAVY
COMMANDER, NAVY INSTALLATIONS COMMAND
716 SICARD STREET, SE, SUITE 1000
WASHINGTON NAVY YARD, DC 20374-5140

CNICINST 2000.1A
N6
10 January 2013

CNIC INSTRUCTION 2000.1A

From: Commander, Navy Installations Command

Subj: GOVERNING POLICY FOR CNIC GATEWAY 2.0 AND ENTERPRISE INFORMATION MANAGEMENT

Ref: (a) OPNAVINST 5450.339
(b) CNICINST 5211.1
(c) SECNAV M-5510.36
(d) SECNAV M-5210.1

Encl: (1) CNIC Gateway 2.0 Business Rules

1. Purpose. To publish the revised policy for the Commander, Navy Installations Command (CNIC) portal, Gateway 2.0 (G2), per reference (a), (b), (c) and (d). This revision refreshes the strategy, policy, guidelines, and responsibilities across the CNIC enterprise for the storage and sharing of unclassified information up to and including controlled unclassified information (CUI).

2. Cancellation. CNICINST 2000.1 dated 28 August 2007.

3. Background. As described in reference (a), Department of Navy (DON) Office of the Chief of Naval Operations (OPNAV) tasks CNIC to manage the Navy’s total shore operating costs, find innovative solutions to control and mitigate those costs, and develop shore readiness. This requires implementing guidance in coordination with Navy component commanders to mitigate impacts, ensure operational readiness and resourcing, and maintain reliable, accurate, and authoritative data and information systems. In addition, CNIC is required to define performance levels and metrics and establish business tools that standardize practices and oversight. To that end, the command fully embraces technology platforms as the enabler to revolutionize CNIC’s approach to enterprise structure, process, and training integration. CNIC’s central technology platform is G2. G2 is CNIC’s single on-line environment designed to encompass all relevant information across CNIC’s business lines and products,

with appropriate relevance to installations, regions, and customers to enable staff to conduct business, measure and manage organizational performance, locate subject matter experts, and collaborate and innovate. G2 includes a structured enterprise data warehouse (EDW) to encompass all of CNIC's business lines and products. The EDW comprises a suite of dynamic collaboration features providing the ability to seamlessly interact across functions and geographies. Features such as profiles, instant messaging, wikis, and more increase the speed of communication and decision making across the command, enabling the delivery of effective services more efficiently.

4. Policy

a. CNIC's G2 is the standard for content management, collaboration, business management processes, and organizational metrics across the command. G2 has eliminated the need for many legacy applications and is an integration path for existing applications as identified by CNIC. All of CNIC, its subordinate commands, partners, tenants, and their personnel will have access to G2. It will be utilized to fulfill CNIC business needs including content management, collaboration, document storage, document search, workflow, strategic communication, business process management, region intranet and extranet sites, and application integration.

b. The CNIC G2 is for unclassified information only, including controlled unclassified information (CUI). Anything posted on G2 could be considered discoverable information in a court of law and could be used for litigation purposes. Content found on G2 that is deemed inappropriate could subject the content provider to appropriate disciplinary action.

c. Effective upon receipt, region commanders (REGCOMs), installation commanding officers (COs), N-Code Directors/Special Assistants (SAs), and individual users are responsible for ensuring that the policy, procedures, and requirements of this instruction are adhered to with respect to the use of G2. Responsibility for implementation of this policy rests with the CNIC Chief Information Officer.

5. Responsibilities

a. CNIC headquarters (HQ) Information Technology (N6) is responsible for:

(1) Managing overall G2 operations.

(2) Designating a CNIC HQ G2 Operations and Leadership Group composed of the CNIC Chief Information Officer (CIO), the Deputy CIO, N6 Application Support (N62) Branch Head, Enterprise Information Management (EIM) (N63) Branch Head, and additional representatives as necessary.

(3) Designating a CNIC G2 Enterprise Support Center (ESC) as the centralized help desk for G2 user support.

(4) Designating a CNIC G2 Operations Support Group (OSG) to support the operation and maintenance of the hardware and software that compose G2.

b. CNIC HQ G2 Operations and Leadership Group is responsible for:

(1) Ensuring proper alignment between business management, technology management, and strategic communications for CNIC.

(2) Meeting as required to discuss various G2 issues and take action as appropriate.

(3) Reviewing the G2 structure and providing technical insight in selecting platforms, network architecture, system software, and security.

(4) Coordinating as appropriate with N-Codes/SAs and providing insight on technical direction for the relevant business areas.

(5) Managing and maintaining the EIM Capabilities Development Framework, which provides a set of processes and procedures that govern the development of business capabilities for G2. Framework documents are posted to Help Central on the N6 G2 teamsite at https://g2.cnic.navy.mil/cnichome/Pages/HelpCentral.aspx.

(6) Ensuring CNIC HQ, regions, and installations have a means to successfully integrate business solutions within G2 and leverage existing standards and tools to develop EIM capabilities.

(7) Providing standard methodologies, development guidelines, and processes to ensure consistency across EIM projects and EIM operations.

c. CNIC G2 Enterprise Support Center (ESC) is responsible for:

(1) Serving as the centralized help desk for all user support for G2.

(2) Providing G2 access management, performance management, as well as general assistance.

(3) Escalating technical issues to the CNIC G2 OSG and forwarding management issues to the Enterprise Gateway Master (EGM).

(4) Providing supporting metrics and information to the CNIC G2 OSG to ensure effective management of the Gateway service-level agreement (SLA).

d. CNIC G2 Operations Support Group (OSG) is responsible for:

(1) Providing G2 software and hardware maintenance, technical consultation, system administration, and infrastructure support, and assisting with the integration of applications into G2.

(2) Serving as primary point of contact (POC) for CNIC G2 system administration and technical issues that cannot be handled by the G2 ESC.

(3) Ensuring documents and electronic evidence are preserved as soon as a party reasonably anticipates litigation, to minimize the risk that potentially relevant evidence is inadvertently or intentionally destroyed and to avoid court sanctions. Questions regarding the preservation of classified materials should be directed to CNIC HQ Office of General Counsel (OGC) or Force Judge Advocate (FJA).

(4) Reviewing the G2 structure and providing technical insight on selecting platforms, network architecture, system software, and security.

(5) Coordinating as appropriate with N-Codes/SAs and providing insight on technical direction for the relevant business areas.

(6) Supporting the integration of identified enterprise legacy applications that require access via the CNIC Gateway.

(7) Providing technical information relative to CNIC Gateway configuration and with development of EIM business solutions.

(8) Supporting the establishment of CNIC G2 sites and work areas for N-Codes/SAs and cross-functional teams (CFTs).

(9) Supporting the management of CNIC G2 area permissions and creating all site structures within the platform with the exception of the team space areas.

(10) Supporting Region Gateway Masters (RGMs) in the establishment of region G2 spaces, taxonomy, and configurations.

(11) Assisting with the migration of legacy content and management systems into G2.

(12) Drafting SLAs.

(13) Developing and maintaining a system recovery plan.

e. CNIC Enterprise Gateway Master (EGM), who resides within N63, is responsible for:

(1) Overseeing the day-to-day execution of the G2 governance policy, understanding strategic and business parameters, and integrating these guidelines into the G2 governance policy and strategy.

(2) Developing, executing, and monitoring all aspects of the CNIC G2 governance policy.

(3) Defining milestones and metrics with the G2 Operations and Leadership Group and renewing the Gateway

strategy as required and providing reports to the G2 Operations and Leadership Group on milestone and metrics progress.

(4) Coordinating as appropriate with N-Codes/SAs and providing insight on technical direction for the relevant business areas.

(5) Supporting the HQ G2 Operations and Leadership Group in preparing analysis and materials for meetings.

(6) Conducting organizational impact planning and coordinating specific change management communication activities.

(7) Developing and executing a G2 communication and training plan.

(8) Meeting with stakeholders and users to understand requirements and communicate available solutions and G2 functionality.

(9) Managing the various levels of training for CNIC personnel, RGMs, CNIC leadership, and other user communities.

(10) Developing the necessary program requirements (personnel, hardware/software, and other resources) for submittal to the G2 Operations and Leadership Group.

(11) Overseeing the activities of the G2 OSG and the G2 ESC.

(12) Facilitating the stand-up and productivity of the Communities of Practice (COPs).

(13) Coordinating the actions of the HQ Gateway Master (HGM), RGMs, content managers, and users.

(14) Facilitating the capture, distillation, and application of best practices and lessons learned.

(15) Coordinating, consolidating, and communicating the activities of the RGM Working Group (RGMWG).

f. HQ Gateway Master (HGM) is responsible for:

(1) Chairing the RGMWG and facilitating working group meetings.

(2) Supporting the EGM in disseminating lessons learned and best practices.

(3) Performing all of the functions of the RGMs described in paragraph 5.l, for the HQ community.

(4) Operating and maintaining G2 Help Central, the help area on G2 dedicated to providing G2 assistance and training.

(5) Recommending approaches and standards for content management, taxonomy, and metadata.

g. HQ Content Managers (HCMs) are responsible for performing all of the functions of the region content managers (RCMs), listed in paragraph 5.m, for the HQ community.

h. Region Commanders (REGCOMs) are responsible for championing the lead of the CNIC Gateway within the region to ensure that this instruction is properly implemented to support G2 strategic communications throughout the region.

i. Region Gateway Master Working Group (RGMWG) is responsible for:

(1) Ensuring proper alignment between business management, technology management, and internal communications in G2 implementation within the region.

(2) Ensuring appropriate team membership and representation are established within the regions and installations.

(3) Meeting on a weekly basis, or as required, to discuss various regional Gateway issues raised by the installation COs, program directors, and RCMs, and report findings to the G2 Operations and Leadership Group or to region N-Codes/SAs, as appropriate for the action recommended.

(4) Providing the G2 Operations and Leadership Group with suggested improvements to G2 structure, platforms, network architecture, system software, and security.

(5) Coordinating with region N-Codes/SAs and providing insight on technical direction for relevant business areas as appropriate.

(6) Assisting with the implementation of additional software functionality within G2, including workflow capability, business analysis tools, and records management.

(7) Ensuring that regional issues, concerns, or suggested improvements are addressed in a timely fashion.

j. Installation COs are responsible for ensuring that this instruction is properly implemented in support of content management, collaboration, and strategic communications at their installation.

k. Region N-Code Directors/SAs are responsible for:

(1) Assisting the REGCOMs and installation COs in executing G2 policy and installation programs.

(2) Providing N-Code/SA-specific guidance to RCMs for developing and managing G2 content.

(3) Working with their respective RGMs to designate RCMs for their area of responsibility.

l. Region Gateway Masters (RGMs), appointed by region N6s, are responsible for:

(1) Providing limited technical support for G2 and designated G2 workspaces within their region.

(2) Providing information support and guidance and disseminating the developed CNIC Gateway policy within their region.

(3) Creating, modifying, and removing specific library, list, or document settings or permissions as necessary to support region business requirements.

(4) Migrating content from other data storage systems, including shared drives, local drives, and Clearinghouse, to G2.

(5) Educating RCMs on use of G2 to store and share content from their own programs and communities.

(6) Organizing, updating, and communicating changes to the content management process, strategic objectives and

deadlines, roles and responsibilities, and CNIC Gateway requirements.

(7) Creating G2 groups as necessary to meet business requirements of the region.

(8) Ensuring compliance with CNIC Gateway 2.0 Business Rules as set out in enclosure (1), and maintaining and refining the taxonomy of, and incorporating business requirement information into, G2 search capabilities.

(9) Identify and designate RCMs.

(10) Engaging with OGC and FJA to ensure questions regarding the preservation of classified materials are appropriately handled and accurately answered.

(11) Engaging with the CNIC HQ records manager or region records manager to ensure questions regarding the preservation of documentary materials, specifically records and reference materials, meet Federal and Department of Navy (DON) regulations.

(12) Meeting with RCMs to communicate changes in policy and usage and hear concerns and issues.

(13) Overseeing the training of region personnel and RCMs, as identified.

(14) Providing recommendations or suggestions for improvement to the RGMWG.

(15) Building out G2 site structure for the RCMs using approved G2 site templates.

(16) Identifying, communicating, and recording G2 feedback and issues to appropriate G2 team members for resolution.

(17) Monitoring content for unauthorized collection or maintenance of personally identifiable information (PII) in compliance with reference (b).

m. Region Content Managers (RCMs) and installation Content Managers (ICMs), identified and appointed by region/installation N-Code Directors/SAs, are responsible for:

(1) Managing areas of responsibility that may be at the region N-Code level, region sub-N-Code level, or installation level.

(2) Maintaining a specific area within G2.

(3) Maintaining overall authority for the content on their G2 area to ensure up-to-date, accurate, and appropriate information.

(4) Assisting with ensuring that all files uploaded into their assigned G2 areas contain no classified information, and that information requiring special handling, such as information subject to the Privacy Act or contract-sensitive information, is stored in the controlled access area of G2 and appropriate permissions are in place.

(5) Ensuring records and record data are archived in an approved electronic records management application, e.g., Total Records Information Management (TRIM).

(6) Managing document libraries, metadata, local configuration settings, and local taxonomy.

(7) Approving or rejecting content to be posted to their G2 area and coordinating with users to remove inappropriate content.

(8) Providing user feedback to management to improve G2 operation.

(9) Determining or validating access needs to their area of G2.

(10) Notifying their RGM of personnel changes, and ensuring employees or users have been added or separated, or are no longer with the organization.

(11) Monitoring content for unauthorized collection or maintenance of PII in compliance with reference (b).

n. G2 users are responsible for:

(1) Using G2 to maintain and access data, information, and knowledge required to execute their job responsibilities.

(2) Ensuring that only appropriate unclassified information is placed within the G2 environment and that restricted-access information (Privacy Act, contract-sensitive, etc.) is properly stored and controlled.

(3) Contributing content to G2, participating in G2 learning events, and collaborating with relevant teams.

(4) Ensuring records and record data are archived in an approved electronic records management application, e.g., TRIM.

(5) Using only the tools provided in G2 to make changes to their departmental site on G2. All changes in templates, upper-level permissions, and navigation shall be socialized through the respective content manager for the departmental site, and reviewed and approved by the RGM.

(6) Contacting the appropriate content manager to request permissions for access to any of their departmental documents.

(7) Managing and maintaining the content on their personal G2 workspace in accordance with enclosure (1).

6. Action

a. HQ, region, and installation N6s shall:

(1) Provide G2 subject matter experts to support the governance and management processes identified within this instruction.

(2) Identify and assign RGMs and RGMWG membership.

(3) Contribute to the adoption and implementation of best practices within G2.

b. HQ, region, and installation N-Codes/SAs shall:

(1) Review and adhere to the business rules associated with this instruction (enclosure (1))

(2) Contribute to the adoption and implementation of best practices within G2.

(3) Assign appropriate G2 content managers as identified within this instruction, to ensure program content is accurate, accessible, and housed within the appropriate G2 location.

(4) Provide N-Code/SA-specific guidance to RCMs for developing and managing G2 content.

(5) Leverage the CNIC Support Center to report G2 trouble calls and issues.

c. REGCOMs shall ensure this instruction is properly implemented to support strategic communications throughout the region.

d. Installation COs shall ensure this instruction is properly implemented in support of content management, collaboration, and strategic communications at the installation.

7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed in accordance with reference (d).

W. D. FRENCH
Vice Admiral, U.S. Navy

Distribution:
Electronic only, via Gateway 2.0
https://g2.cnic.navy.mil/CNICHQ/Pages/Default.aspx

CNIC GATEWAY 2.0 BUSINESS RULES

The CNIC Gateway 2.0 Business Rules are established to govern the use of the Commander, Navy Installations Command (CNIC) portal, Gateway 2.0 (G2). Business rules are based on industry best practices, CNIC leadership decisions, CNIC Gateway specifications, and common sense approaches that accommodate the CNIC business environment.

As the principal information exchange medium, CNIC G2 is configured to address a wide variety of user information requirements and to minimize the need for users to go outside of the Gateway infrastructure to satisfy their information-sharing and collaboration needs.

The CNIC Gateway hierarchy shall be based on the CNIC headquarters (HQ), region, installation, and N-Code structure.

The CNIC Gateway is the proper area for all-hands type content, including new policies and procedures, and announcements. The following identifies the business rules for each of the functional areas of the CNIC Gateway.

1. GENERAL RULES

a. CNIC Gateway Information and Contacts. The CNIC Gateway is accessible from any computer with a valid Department of Defense (DoD) public key infrastructure (PKI) certificate at https://g2.cnic.navy.mil. For CNIC users, access is automatically available if the user is assigned or associated to a CNIC uniform industrial code (UIC) in Total Workforce Management Services (TWMS). For non-CNIC users, access should be requested at https://g2reg.cnic.navy.mil/.

b. Additional assistance is available from the CNIC Enterprise Support Center (ESC). Contact is by phone at 1-888-CNI-4ALL or via email at cnicg2support.fct@navy.mil.

c. All CNIC employees shall have access to the CNIC Gateway.

d. The CNIC Gateway is for unclassified information only, including controlled unclassified information (CUI). Anything posted on G2 could be considered discoverable information and may be used for litigation purposes.

e. Users who inadvertently upload a classified document into the CNIC Gateway should immediately follow the requirements detailed within section 12-2 of SECNAV M-5510.36, Department of Navy (DON) Information Security Program, dated June 2006. In addition, they should also notify their Region Gateway Master and the ESC via phone at 1-888-CNI-4ALL or email at cnicg2support.fct@navy.mil. Select ”Software and Application Support,” followed by ”CNIC Gateway and CNIC Website Support.”

f. The CNIC Gateway is the primary method of strategic communication, information sharing, and collaboration for the CNIC workforce.

g. Gateway Masters and other Gateway management team members shall be given authorization to modify permission settings based upon specific mission requirements.

h. The CNIC Gateway hierarchy taxonomy shall be based on the CNIC HQ, region, installation, and N-Code structure, functions, and business outputs/products.

i. The CNIC Gateway shall be used for official government business only. Personal advertisements and the promotion and sale of goods and services not related to CNIC business are not permitted on the CNIC Gateway. Content found on the Gateway that is deemed inappropriate could subject the content provider to appropriate disciplinary action.

j. HQ Gateway Master (HGM) and Region Gateway Masters (RGMs) shall designate an alternate who will act when the primary Gateway Master is unavailable. HGM and RGMs and their alternates shall provide contact information while away from the workplace. The Region Gateway Master shall notify the HQ Gateway Master or the CNIC Enterprise Gateway Master (EGM) of any changes to RGM assignments. Changes in assignments of RGM personnel shall be reviewed by the EGM.

k. Users should follow U.S. Navy approved naming conventions when naming files: [REGION]_[N-Code]_[Title]_[Version]_ [DDMMMYY] (e.g., HQ_N63_G2_Business_Rules_Final_11SEP12).

l. There shall be a central location on G2 for all governing policy and business rules updates. These policies and rules shall be reflected through Help Central, the help area on the Gateway dedicated to providing G2 assistance and training, and promulgated through Region Gateway Master communication channels. Users shall be informed when there is a change to governing policy or business rules affecting the way they do business through their respective content managers and Region Gateway Masters.

m. Users should practice version control when placing files in the Gateway document library. This includes posting each file to a single library rather than to multiple libraries, and following the approved taxonomy. Users shall limit the number of versions retained. Versioning should be set to allow up to three major versions and no minor versions.

n. Users should maintain documentation on G2 and, when sharing documents with CNIC employees or anyone else with access to the CNIC Gateway, should send a notification email to potential users with a hyperlink to the document rather than using email attachments. Any hyperlink provided should directly link to the document for the convenience of the recipient, as files can be difficult to locate without this guidance.

2. CONFIGURATION MANAGEMENT

a. The G2 Operations and Leadership Group, following an established change control process, shall review change control requests to determine viability, priority, and scheduling.

b. CNIC Gateway architectural changes, such as expansion and migrations, shall be reviewed by the Enterprise Gateway Master or the G2 Operations and Leadership Group to determine and minimize system down-time.

3. ADMINISTRATION AND SECURITY

a. The G2 Operations and Leadership Group shall annually review the structure (i.e., organization, system architecture, application portfolio, taxonomy, etc.) of the CNIC Gateway, preferably in conjunction with the change of the fiscal year. The CNIC Gateway shall not change structure until such a review has been conducted.

b. Site access and permissions guidelines shall be standardized CNIC enterprise-wide under the management of the HQ Gateway Master and Enterprise Gateway Master.

c. Information containing personally identifiable information (PII) must be captured, contained, and appropriately safeguarded within the controlled access (CA) area within G2.

d. HQ, region, and installation security staff shall annually review the CNIC Gateway content to ensure compliance with applicable information security policies.

4. SITE ADMINISTRATION MANAGEMENT

a. A public CNIC Gateway landing site shall be created for HQ, and all regions, installations, and N-Codes. Public landing pages shall be created for select initiatives as designated by CNIC leadership and required by CNIC products and services. These sites and pages shall be accessible to all CNIC employees, registered non-CNIC G2 users, and users with valid DoD Common Access Cards (CACs). Public landing pages shall be used for the dissemination of general information such as Commander's comments, general announcements, common links, VIP profiles, common instructions, general information and general training aids.

b. An Organization Team Site shall be created for HQ and all regions, installations, and N-Codes. These sites shall be accessible to all CNIC employees and registered non-CNIC G2 users. CNIC employees who are members of the region shall have contribute rights to the top-level organizational team site and the N-Code-level team site for their respective region. Content generally shall be accessible to all registered G2 users unless there is a reason to restrict access. Permissions and access for sub-N-Code sites and content may vary in accordance with the discretion of the Region Gateway Master. The Organization Team Site shall be used for dissemination of day–to-day information and work products and the execution of business processes, to members in their region and across the regions. It should be noted that cross-collaboration between regions should be facilitated elsewhere as read access is the default permission for any user outside of the region.

c. The HQ Gateway Master, Region Gateway Masters, and content managers at all levels are responsible for the organization and content of these public landing sites and Organization Team Sites. They shall monitor content for unauthorized collection or maintenance of PII in compliance with CNICINST 5211.1, the CNIC Privacy Program. They shall also ensure that Department of Navy (DON) records are archived in an approved electronic records application, e.g., Total Records Information Management (TRIM).

e. My Workspace Team Spaces shall be used mainly for cross-collaboration between N-Code teams, project teams, and region teams. Project leaders requiring a team space for their team shall be able to provision a team space using services provided in the My Workspace area or by requesting their respective Region Gateway Master to set it up and provide tips on usage. Any team spaces set up for projects shall be archived or deleted upon completion of the project. If records are created in a team space, they need to be archived in an approved electronic records application, e.g., TRIM.

f. Private content can be added by individual users to their My Workspace area to best meet their needs. Items accessed on a recurring basis, such as links and current documents, should be placed on the user's My Workspace area.

g. The profile area under My Workspace shall communicate specific information to all CNIC Gateway account holders, such as contact information, subject matter expert information, colleague connections, and recent public postings. Data stored on this area shall be available to all users via the search function and through the user’s electronic business card which is accessible wherever their account name is displayed on the Gateway.

h. Once personnel are no longer members of the CNIC organization, any files they had placed on the CNIC Gateway shall be purged or transferred to another user, as appropriate, by their organization, in a manner to be determined by the Region Content Manager and executed by the Region Content Manager’s designated agent.

5. WEB CONTENT MANAGEMENT

a. All training, usage, and general CNIC Gateway help information shall be organized logically in the CNIC Gateway Help Central. All regions shall link to this area as the main Help document library. The Help Central shall be maintained by the HQ Gateway Master and the Enterprise Gateway Master. Any suggested changes may be sent to them for posting. A CNIC HQ staff member shall be designated as the content manager for the Help site.

b. Each user shall manage the content on his or her personal CNIC Gateway Workspace.

c. HQ or region business surveys created within G2 shall be loaded to an appropriate area of the CNIC Gateway for their target audience, or appropriately linked if the survey was not created using the CNIC Gateway survey tool.

d. G2 shall not be used for unofficial data or files that would limit CNIC server space for official data. Examples of unsuitable files or data are personal pictures, music, jokes, recipes, etc. Corrective action shall be taken by CNIC Region Gateway Masters to ensure that all data in the CNIC Gateway complies with the guidelines set forth in this document.

e. The HQ Gateway Master shall establish standard web parts and links that are used across the CNIC enterprise, which may be accessible from the CNIC home page or region home pages, or within departmental areas.

f. There shall be a common area on each region Gateway site for all-hands information. Every user shall automatically have at least read rights to this area. This area shall have links to pre-determined sites common to the business functions, such as Standard Labor Data Collection and Distribution Application (SLDCADA), Defense Travel System (DTS), and CNIC instructions.

g. Departmental sites shall have links to U.S. Navy web sites and web applications relevant to those sites, such as facilities linking to Internet Navy Facilities Asset Data Store (iNFADS) and Casualty Assistance linking to the Casualty Assistance Calls Office (CACO) database. The Region Gateway Master shall coordinate with the N-Codes/SAs to determine what links shall be added to the specific areas.

h. The public landing page on each region Gateway site shall include links to reference materials established by the G2 Operations and Leadership Group for consumption by CNIC enterprise-wide.

i. Content managers and users shall report complaints and issues to their Region Gateway Master and the Enterprise Support Center. Content managers shall meet periodically with their respective Gateway Master to identify continuing issues or complaints and determine possible solutions.

6. DOCUMENT MANAGEMENT

a. The naming convention for files posted to the CNIC Gateway shall use logical, standard naming conventions. For example, a Word file for business rules will be labeled “HQ_N63_G2_Business_Rules_Final_11SEP12” using a standard format of region, N-Code, document title, version, and date, separated by an underscore: [Region] _N-Code]_[Title]_[Version]_[DDMMMYY].

b. File types that are listed in the default Restricted File Type list will be blocked from upload to G2. All executable file types (.exe) are restricted. The size limitation on single-document uploads shall be 100 megabytes (MB). Exceptions will be handled on a case-by-case basis.

c. All files requiring limited access shall be uploaded directly to an area on G2 with the appropriate access restrictions. If a user does not know the restrictions of an intended area, please consult with the respective Content Manager or Region Gateway Master.

d. Users are responsible for cleaning up and purging files and information that are no longer required. Users are also responsible for ensuring that DON records are maintained in accordance with the retention guidelines in the DON Correspondence Manual, SECNAV-M 5210.1.

7. TAXONOMY. The CNIC Gateway hierarchy taxonomy shall be based on the CNIC N-Code structure, functions, and business outputs/products.

8. EMAIL. The use of email for distribution of large documents, all-hands messages, or CNIC-wide information should be limited. Users should place large documents within the appropriate area of the CNIC Gateway then provide users with the link to the document. The use of common areas within G2 to disseminate all-hands or CNIC-wide information is highly recommended.

9. TRAINING. The CNIC Gateway training process, as defined and developed by the Enterprise Gateway Master, provides training at all levels for Gateway Masters, Content Managers, and users. Periodically, training by the Region Gateway Masters shall be provided for Region Content Managers and users. Content Managers shall be trained on document review, adding and removing access to their areas, and adding lists and document libraries. Content Manager training shall include proper handling of PII and records management. Part of the Content Managers' responsibilities shall be to assist users with their departmental sites.

10. BEST PRACTICES. Best practices will be made available to all users in the CNIC G2 Help Central. All users of the Gateway are encouraged to contribute their best practices via their respective Gateway Master or Content Manager.

11. SECURITY GROUPS

a. Active directory, Gateway, site, and cross-site security groups shall be utilized for managing site access and permissions. These security groups shall be assigned roles within the CNIC Gateway and site structure as applicable, and shall be monitored by the HQ Gateway Master, Region Gateway Masters, or Content Managers.

b. Enterprise Level. CNIC Gateway area permissions shall be managed by the HQ Gateway Master and the Enterprise Gateway Master. The HQ Gateway Master shall also be responsible for creating all top-level team sites.

c. Region Level. Regional site permissions shall be managed by the Region Gateway Masters. The Region Gateway Masters shall be responsible for sub-site creation through the existing G2 team site request process.