DEPARTMENT OF THE ARMY
U.S Army Signal Center of Excellence
506 Chamberlain Avenue
Fort Gordon, Georgia 30905

REPLY TO
ATTENTION OF

ATZH-KM 25 August 2012

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Management of Signal Center of Excellence (SIGCOE) Web Sites

1. References.

a. AR 25-1, Army Knowledge Management and Information Technology, 4 December 2008.

b. AR 25-55, Army Freedom of Information Act Program, 1 November 1997.

c. AR 340-21, The Army Privacy Program, 5 July 1985.

d. AR 360-1, The Army Public Affairs Program, 15 September 2000.

e. AR 380-5, Department of the Army Information Security Program, 29 September 2000.

f. AR 530-1, Operations Security (OPSEC), 19 April 2007.

g. Department of the Army (DA) Pamphlet 25-1-1, Information Technology Support Services, 25 October 2006.

h. Department of Defense (DoD) Directive 5205.02, DoD Operations Security (OPSEC) Program, 6 March 2006.

i. DoD Directive 5230.09, Clearance of DoD Information for Public Release, 22 August 2008.

j. DoD Publication 8910.1-M, DoD Procedures for Management of Information Requirements, 30 June 1998.

k. DoD Instructions 5230.29, Security and Policy Review of DoD Information for Public Release, 8 January 2009.

l. DoD Web Site Administration Policies and Procedures, 25 November 1998.

2. Purpose. This policy provides specific guidance on the enterprise-wide business process for establishing, operating, and maintaining SIGCOE web sites.

3. Proponent. The proponent for this policy is the SIGCOE KM, Knowledge Management Office (KMO).

4. Policy.

a. This policy is overarching in nature and applies to all SIGCOE organizational elements.

b. Using the Internet (World Wide Web) is strongly encouraged in that it provides the SIGCOE with a powerful tool to convey information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies, and programs.

c. The considerable mission benefits gained by using the web must be carefully balanced against the potential risk to SIGCOE interests, such as the safety and security of personnel and assets or individual privacy, as well as ensuring that all websites properly align and convey the SIGCoE Strategic Vision and Campaign Plan.

5. Definitions.

a. Home Page. The index or introductory document for a web site.

b. Internal Collaboration Portal. A SharePoint site used internally to the SIGCoE for staff to collaborate and disseminate information.

c. Intranet. See also Internal Collaboration Portal.

d. Official DoD Web Site. A DoD web site that is developed and maintained with command sponsorship and approval, and for which the DoD Component, a subordinate organization or individual, exercises editorial control over content. The content of official DoD web sites is of an official nature that may be endorsed as the official position of the DoD Component. Content may include official news releases, installation history, command position papers, etc. Official DoD web sites are prohibited from displaying sponsorships or commercial advertisements.

e. Page Administrator / Content Manager. This person is responsible for a web page. This responsibility includes all facets of a web page including, but not limited to, the functionality of a web page, as well as the data contained on that page.

f. Publicly Accessible Web Site. A web site that contains releasable information and is accessible to the general public over the Internet.

g. Web Page. A document on the World Wide Web (Internet). Every web page is identified by a unique Uniform Resource Locator (URL).

h. Web Portal. A web site that offers a broad array of resources and services, such as e-mail, forums, and search engines.

i. Web Module or Widget. A small, self-contained window within a web portal that displays useful information or offers a relevant service.

j. Web Program Manager. This person is the single point of contact for all issues associated with the web site. The Web Program Manager has technical control over the site's content and ensures the site conforms to DoD and Army web site requirements.

k. Web Site. A site (location) on the World Wide Web. Each web site contains a home page, which is the first document users see when they enter the site. The site might also contain additional documents and files. Each site is owned and managed by an individual, company, or organization.

6. Responsibilities.

a. Servicing Public Affairs Officer (PAO).

1. In concert with the SIGCOE KM TEAM, provide oversight and review of the content on the SIGCOE public web site.

2. Establish a process for the identification of information appropriate for posting to the publicly accessible web site and ensure it is consistently applied.

3. Ensure the review of information for security, levels of sensitivity, and other concerns before release.

4. Ensure the accuracy, consistency, appropriateness, and timeliness of all information placed on the web site.

5. Conduct quarterly review of all SIGCOE and subordinate sites for compliance with established guidance for appropriateness of information. The PAO will notify the Web Program Manager and Page Administrators/Content Managers of any non-compliant information.

6. Ensure the establishment of procedures for management oversight and regular functional reviews of the web site.

b. SIGCOE KM TEAM.

(1) Appoint an SIGCOE Web Program Manager (Certified IA Compliant Webmaster). This person is the single point of contact for all issues associated with the web site.

(2) Establish a service agreement with the Fort Gordon Network Enterprise Center (FGNEC) for the technical development, operation, and maintenance of the SIGCOE web server. The FG NEC is the designated single source for web hosting, establishment, operation, and maintenance of SIGCOE public web sites.

(3) Eliminate unnecessary and/or inefficiently operated web sites to reduce operating costs.

(4) Establish a plan for the migration of legacy web content to the approved SIGCoE Branded Template and Framework. Site must be currently maintained and updated within the last 12 calendar

month to be considered. For more information on the approved SIGCoE tempate based on the ARMY standard Template please follow this link: (https://cac.tkeportal.army.mil/sites/signal/default.aspx)

(5) Provide policy and procedural guidance with respect to establishing, operating, and maintaining SIGCOE web sites.

(6) Approve and publish instructions and publications, as necessary, to guide or direct SIGCOE publicly accessible web site activities.

c. SIGCOE Information Assurance Manager (IAM) (G6).

(1) Ensure Internet users are aware of the Internet's vulnerabilities, their individual responsibilities, limitations of access, and the approval process for release of US Government information.

(2) Ensure that approved DoD security and privacy notices and applicable disclaimers are used on all web sites under their purview.

(3) Ensure that a comprehensive, multi-disciplinary security assessment is conducted of the SIGCOE publicly accessible web sites within 120 days of the promulgation of this document and at least annually thereafter.

(4) Maintain the operational integrity and security of the computer and the network supporting the web site.

d. SIGCOE Web Management Team.

(1) Ensure all information placed on publicly accessible web sites is appropriate for worldwide dissemination and does not place national security, DoD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

(2) Conduct quarterly review of all SIGCOE and subordinate sites for compliance with established guidance for appropriateness of information. The SIGCOE KM Office will notify the Web Program Manager and Page Administrators/Content Managers of any non-compliant information.

e. Web Program Manager (Certified IA Compliant Webmaster).

(1) Monitor professional appearance of web pages.
(2) Establish procedures for updates to web site content.
(3) Maintain technical control over the site's content and ensure the site conforms to DoD and Army policies, standards, and conventions.
(4) Apply appropriate privacy and security policies to respect visitor's privacy.
(5) Complete the online Army Web Content and OPSEC Certification Training Course located at https://iatraining.us.army.mil/index.php.

f. Page Administrators/Content Managers.

1) Serve as the Unit level content manager and have design and admin control over a specific we page or site.
2) Request a Page manger Appointment see Appendix d
3) Ensure Page/Site content meets OPSEC and KM requirements (see appendix d)
4) The Page Manager will be required to issue changes though the TKE Help Desk attach changes in .Zip file format via the attach files button on the new ticket
5) ensure that the changes are in lines with the SIGCoE / GARRISON provided templates
6) Any special advanced coding requests are handled on a case by case bases.
7) The Page Manager will ensure the site he/she webpage will be maintained, meet OPSEC and up to date at least quarterly to ensure relevance of information.
8) A automated update notification and verification system including Update procedures and checklist can be found on the TKE Help Desk Home page under sections, Garrison Website and Social Media Inventory or SIGCoE Website and Social Media Inventory. This list should contain the PM's site with relevant contact and OPSEC/Content inspection dates. and Failure to do maintain the webpage or up to date list may result in suspension of services

g. Web Server Systems Administrator.

(1) Maintain web server hardware and software.
(2) Is an IAT II level administrator.
(3) Maintain web server security and administer user rights.
(4) Ensure mechanisms are in place to control access to the SIGCOE publicly accessible web sites as appropriate.
(5) Ensure web servers are Information Assurance Vulnerability Management (IAVM) compliant and placed behind a reverse proxy server, or implement an alternative security procedure.
(6) Ensure compliance with this policy and remove non-compliant sites.

h. Commanders, Chiefs/Directors, or their designated representatives.

(1) Define the purpose of the organization's web site and develop guidance on information to be posted that will be of value to the intended audience.

(2) Appoint directorate/command Page Administrators/Content Managers.

(3) Establish procedures to ensure that classified, Privacy Act information, or information that could enable the recipient to infer classified or unclassified sensitive information is not posted to SIGCOE publicly accessible web sites.

(4) Establish procedures for the periodic review of web pages maintained by their organizations to ensure the content does not adversely affect the SIGCOE.

7. Procedures.

a. Official SIGCoE web sites should be made publicly accessible on the Internet only when the target audience includes the public at large. The KM Team provides quality Official Web products for use by SIGCoE Subordinate units. These website products consist of the following,
   (1) Public Websites **APPENDIX B**
   (2) Event or Conference Websites **APPENDIX C**
   (3) AKO Websites **APPENDIX B**
   (4) Special Official Websites **APPENDIX B**

b. **All Page Managers will meet the requirements outlined in Appendix D**

c. Information that is for SIGCoE personnel only and for an organization's exclusive use should be moved to the SIGCoE TKE SharePoint Portal. SIGCoE TKE portal is the primary source for collaboration and coordination of non-public information. Private (intranet) web sites must migrate to SIGCoE TKE per AR 25-1 and REG.85370. All internal organizations will maximize their use of SIGCoE TKE resources, features, and tools to reduce the need for investment in the same types of IT resources.

d. Information that is for outside of the SIGCoE but not publicly releasable will leverage AKO to the maximum extent possible within the Signal Knowledge Networks and its portals inside AKO. Private web sites separate from AKO should be established only when AKO cannot support the requirement. The use of AKO enables optimal sharing of information and knowledge resources across the entire Army enterprise. All activities will maximize their use of AKO resources, features, and tools to reduce the need for investment in the same types of IT resources.

e. The SIGCOE publicly accessible web sites will be DA accredited and registered with appropriate agencies.

f. The Web Program Manager and Page Administrators/Content Managers will ensure that publicly accessible web sites conform to the SIGCOE web page design standards.

g. All web sites must contain a clearly defined purpose statement that supports the mission of the organization.

h. Each privacy and security notice must clearly and concisely inform visitors to the site what information the activity collects about individuals, why it is collected, and how it will be used.

i. Hyperlinks on SIGCOE web sites to home pages, web sites, or other web resources of a personal or non-mission related nature are prohibited. The Commander may authorize hyperlinks to information on the Internet which provides free public information supporting the organization's mission.

j. Commercial sponsorships, advertisements, and endorsements are prohibited. Organizations shall not post advertisements on publicly accessible web sites. Organizations shall ensure that the credibility of

official information is not adversely affected by association with commercial sponsorships, advertisements, or endorsements.

k. All organizations must follow and comply with the guidelines as set forth in the Accessibility of DoD Web Sites to People with Disabilities Act. Section 508 requires that Federal agencies' electronic and information technology is accessible to people with disabilities, including employees and members of the public. Section 508 establishes requirements for any electronic and information technology developed, maintained, procured, or used by the Federal Government.

l. All SIGCOE web sites will comply with the DoD Web Site Administration Policy that requires that information be reviewed for data sensitivity prior to web posting and protected accordingly.

m. Only official information that is releasable and of value to the public may be posted on Army public web sites. All SIGCOE Web portals containing information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to the SIGCOE, especially in electronically aggregated form, must employ additional security and access controls.

n. Web sites containing information in the following categories should not be accessible to the general public:

(1) Plans or lessons learned that would reveal military operations, exercises, or vulnerabilities.

(2) Personal information about US citizens, DoD employees, and military personnel, to include the following:

(a) Social security numbers.

(b) Dates of birth.

(c) Home addresses.

(d) Directories containing name, duty assignment, and home telephone numbers.

(e) Names, locations, or any other identifying information about family members of DoD employees or military personnel.

o. The use of the SIGCOE web site or other publicly accessible web sites are for official, unclassified, non-sensitive US Government business only. Web sites must be developed with the utmost security applicable when dealing with the privacy of individuals.

(1) Restrictions on release of information:

(a) Classified information is not releasable to the public and will not be posted on web sites.

(b) Unclassified but sensitive information will not be posted on web sites.

(c) Personally identifiable information (PII) is prohibited from being released, in accordance with AR 340-21, and will not be posted on web sites.

(d) Information outside the purview of the commander/director directly responsible for the web site is not releasable to the public without written permission from the proponent. If the material is posted on the proponent's public web site, information must be accessed via a link, not reiterated.

(2) Copyright protected material will not be used on the SIGCOE web site, or on any other SIGCOE publicly accessible web sites, without appropriate authority from the holder of the copyright.

p. Users will provide the highest possible level of data assurance (virus protection) when loading/downloading information to/from web sites. This precludes data being stored, transmitted, or processed in Army computers, systems, or networks from getting infected with malicious logic. Report files with suspected viruses to your Page Administrator/Content Manager and Information Assurance Security Officer (IASO) for verification, reporting, and removal of the virus.

To request a Public, AKO, Website, please follow the Public Website Guidelines and Checklist Appendix B

To request a Event or Conference Site, please follow the Public Conference Website Guidelines and Checklist Appendix C

To request a Webmaster/Admin or Page manager appointment, please follow the Appointment guidlines Guidelines and Checklist Appendix D

q. The SIGCOE KM KMO, SIGCOE IAM, and SIGCOE Web Program Manager will ensure that adequate security is in place. This procedure will prevent the contamination of files, materials, and/or the loss of services on the SIGCOE web site, or other SIGCOE publicly accessible web sites. Firewalls should be external to the Local Area Network to prevent unauthorized access to networks. The SSL must be enabled and PKI certificates installed on all private web sites. Web servers will be behind reverse proxy servers.

r. Any use of the SIGCOE web site, or other SIGCOE publicly accessible web sites, is subject to monitoring without notification to users, systems, or network administration.

s. Users noticing violations of governing regulations should report the violation to the SIGCOE IAM and their direct IASO. The IAM or IASO will report the violations through security channels to the Web Program Manager and initiate corrective action.

t. Each organization with a web site will institute a review process to ensure that information provided on their web sites is current, timely, and cleared for public release. This review process will include, at a minimum, PAO and OPSEC review.

u. If a web page is moved or deleted, especially the homepage or a main section page, Page Administrators/Content Managers should leave a marker page at the old URL to direct and link visitors who may have bookmarked the old page to the new URL.

v. In the event that there is a disagreement as to the appropriateness of specific web content, the Web Program Manager, Page Administrator/Content Manager, SIGCOE IAM, PAO, and G6 OFFICE (OPSEC) will develop a recommendation to the Commander for a decision regarding the posting of the web content.

8. The point of contact for this policy is the SIGCOE KM Team at 706-791-6144.

FOR THE COMMANDER:

X
Quinzel E. Chestnut

QUINZEL CHESTNUT
GS-13
Chief, Knowledge Management

DISTRIBUTION:
A

APPENDIX A
OPSEC Checklist

Operations Security (OPSEC) Checklist for Publicly Accessible Army Websites			
Name:	Date/Time of Review:		
Organization Reviewed:	Primary IP Address/URL:		
Issue/Concern:	***Yes***	***No***	***Notes/Comments:***
Management Controls (Note 1): 1. Does the web site (WS) contain a clearly defined purpose statement that supports the mission of the DoD Component? 2. Is a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each web information service? 3. If applicable, does this WS contain a Disclaimer for External Links notice when a user requests any site outside of the official DoD web information service (usually the .mil domain)? 4. Is this WS free of commercial sponsorship and advertising?			
DEPSECDEF Guidance (Note 2): 1. Operational Information: a. Does the WS contain any information indicating plans or lessons learned which would reveal military operations, exercises, or vulnerabilities? b. Does the WS reference any information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program? 2. Personal Information: Does the WS contain personal information in the following categories about US citizens, DoD employees, and military personnel? - Social Security Numbers			

- Dates of Birth - Home Addresses - Home Telephone Numbers - Names, locations, or any other identifying information about family members of DoD employees or military personnel 3. Technological Data **(Note 3)**: Does the WS contain any of the following technical data? - Weapon Schematics - Weapon System Vulnerabilities - Electronic Wire Diagrams - Frequency Spectrum Data			
OPSEC Considerations: **"Tip Off Indicators" (Note 4):** Does the WS contain relevant information in the following categories that might reveal an organizations plans and intentions? 1. Administrative: - Personnel Travel (personal and official business) - Attendance at planning conferences - Commercial support contracts 2. Operations, Plans, and Training: - Operational orders and plans - Mission specific training - Exercise and simulations activity - Exercise, deployment or training schedules - Unit relocation/deployment - Inspection results, findings, deficiencies - Unit vulnerabilities or weaknesses 3. Communications: - Radio Frequency emissions and associated documentation - Changes in activity or communication patterns - Use of Internet and/or e-mail by unit personnel (personal or official business) - Availability of secure communications - Hypertext links with other agencies or units			

- Family support plans - Bulletin board/messages between Soldiers and Family members 4. Logistics/Maintenance: - Supply and equipment orders/deliveries - Transportation plans - Mapping, imagery and special documentation support - Maintenance and logistics requirements - Receipt or installation of special equipment			
Key Word Search: Use the following key words to conduct a search using the search tool. As a result of this search conduct a random screen of any documents found: - Deployment Schedules - Exercise Plans - Contingency Plans - Training Schedules - Inspection results, findings, deficiencies - Biographies - Family Support Activities - Phone Directories, Lists			

APPENDIX B
Requesting a Public Website for Official Use

Development of Official Public (www), AKO and Special Needs websites

SUBJECT: KM/ GARRISON TEAM WEBSITE DEVELOPMENT SECTION– Public Websites

SIGNAL.ARMY.MIL (SIGCoE/KM Main Web Asset)
GORDON.ARMY.MIL (GARRISON Main Web Asset)
S6.ARMY.MIL (KM CAC-Enabled Primary COP Web Asset)
SLKN.ARMY.MIL (KM Primary CAC-Enabled Web Asset)

SIGCoE KM and US Army Garrison-Fort Gordon/PAO Team designs high quality websites, graphics, coding and other web based content to a high standard in lines with the Army public website, its branding guide and design principles. All web products from the KM/GARRISON design meet stringent design and quality control measures to ensure a quality product that represents the Signal Regiment and Fort Gordon Garrison as a whole; ensuring the SIGCoE and USAG-FG/PAO meet or exceed IA and OPSEC requirements, latest vulnerability patching, technological advancements with proven reliable web and server technologies. The KM/GARRISON Team reserves the right to refuse content that does not meet OPSEC, Mission, Design and Quality Control requirements, as outlined in the guides located on TKE SharePoint KM home page.

Customers Responsibility:

1. The Customer Should request Via the SIGCoE TKE SharePoint HELPDESK (link: https://cac.tkeportal.army.mil/sites/signal/helpdesk), **No Less than 10 business** Days prior to the date in which a website is needed including delivery of all needed materials to be published on the site, included in part 3 below. The customer should have a clear understanding of the mission requirement and support the development through the entire process. The KM/GARRISON Web Design Team will help to determine whether the content is to be public or private. This document covers public facing sites. Please see the SOP for CAC-Enabled Private facing sites on the KM TKE Home page.
2. The Customer assumes the understanding that the Top-Level Administration, sub-development, server and domain requirements will be handled by the KM/GARRISON Team on behalf of the requesting unit.
3. It is the Customers responsibility to provide the following information to the KM/GARRISON TEAM **during the request** of the site to facilitate a high-speed work flow and delivery of product by suspense date.
    - **a.** Unit/Org Page Name
    - **b.** Primary Goal of Website (e.g A place Unit family members can get information)
    - **c.** Primary Website Content
        - **i.** A Power Point slide detailing the Content & Basic Design of the Website, **Note:** That the KM/GARRISON Team will provide a template designed and approved by SIGCoE and USAG-FG/PAO in lines with the U.S. Army website branding guide for any site listed under the Signal.army.mil or Gordon.army.mil websites. The SIGCoE branding guide can be found on the KM/GARRISON team TKE home age

ii. Graphics, Logo's and Pictures (SIGCoE and USAG-FG/PAO Reserve the right to Approve, and/or Re-Design graphics to better represent the Army Branding Guide or the SIGCoE and USAG-FG/PAO Development Policy)

d. Additional Documents that the Website Clients, Customer may need to distribute via a public platform : e.g. "Word/Office docs, PDF's, Registration Email's, etc."

e. Primary and Secondary POC with Primary mail.mil Domain Emails to liaise with the KM/GARRISON Team for Site development, general questions and problem resolution. The Page Managers will have to meet minimum requirements outlined in the attachment provided.

i. Page Manager Requirements see Attachment A

f. The Customer will meet the minimum quarterly change requirements to ensure the page is relevant and not abandoned. Failure to properly update a site may result in suspension of services. It is not the responsibility of the KM/GARRISON Team to ensure sites are up to date.

KM/GARRISON TEAM:

1. The KM/GARRISON Team Shall Provide one public website per request 4 weeks after the appropriate content is provided, (based on mission requirements)
2. The KM/GARRISON Team will provide a website consisting of:
    a. One personalized site or page on Sub or Top Level domain
    b. Placement of graphics pertaining to the Unit in lines with the SIGCoE and USAG-FG/PAO Main Page Template. (Title, Logo, etc.)
    c. Information Pages:
        i. Front Page with Welcome Note and Graphics Placed
        ii. Unit Specific Navigation Bar
        iii. Pages to extra content or purpose
    d. One Primary KM/GARRISON Webmaster and Site POC for general design and problem resolution
    e. Army Policy Links, Declaimers, 508 Compliance and Notices as Per Army Regulation 25-1
    f. Analytics monitoring and Usage reports
    g. Maintenance of the Web Server environment and technologies by serving as the POC and Technical leads to liaison with the Network Enterprise Center (NEC) on the customers behalf.
    h. Ensuring any technologies/websites/pages/environment are functioning properly and meet the customers mission
3. The KM/GARRISON Team will issue patches, major changes and quarterly updates on a regular basis in regards to branding, templating, coding specific SIGCoE / DOD / Army requirements and needs. In addition the KM/GARRISON Team will apply the latest technology is and ensure IA , development policy, security, server environment / status and QA requirements; as well as new modules and widgets will be developed and available.

4. Serve as the Administrative POC, Support and Technical Leads for any site content changes, design issues, functionality issues, and Security & OPSEC concerns.

Please fill out the ticket form located at: https://cac.tkeportal.army.mil/sites/signal/helpdesk to request a site.

APPENDIX C
Requesting a Public Event or Conference Website for Official Use

Development of Conference, Special Needs or Event Websites

SUBJECT: Generic Conference/Event Sites

Customers Responsibility:

1. The Customer Should requests Via the SIGCoE TKE SharePoint (link: https://cac.tke.army.mil/sites/signal/) , **NLT** 31 Days prior to the Conference or Event date in which a website is needed for marketing and information distribution purposes.
2. The Customer assumes the understanding that the development will be handled by the KM Team on behalf of the requesting unit.
3. It is the Customers responsibility to provide the following information to the KM / STRAT COM TEAM ASAP during the request of the site to facilitate a high-speed work flow and delivery of product by suspense date.
    - **a.** Conference/Event Name
    - **b.** Primary Location
    - **c.** Security Status (Public/Private/Special Needs)(Note: The KM / STRAT COM Office does not provide security clearance verification services or facilities arrangements)
    - **d.** Event Date and Time
    - **e.** A Power Point slide detailing the Conference or Event Schedule , uniform requirements and other important event specific info i.g Location if different from Main location
    - **f.** Additional Documents that the Website Clients, Conference Visitors, Customer may need to distribute via a public or private platform : i.g "Day 1 Main Event Notes.doc"
    - **g.** Primary and Secondary POC with Primary us.Army.mil Domain Emails for Site Event Registration Requests, and to answer general questions about the event via email from website visitors
    - **h.** Primary and Secondary POC to liaise with the KM Team for Site development , general questions and problem resolution

KM TEAM:

1. The KM Team Shall Provide One Conference or Event Website per request NLT 2 week after the request is submitted by the customer and the appropriate content is provided.
2. The KM / STRAT COM Team will provide a template consisting of:
    a. One Custom Website with Signal.Portal Domain
    b. Placement of graphics pertaining to the event. (Title, Logo etc)
    c. Information Pages:
        i. Registration Page with Web Form to handle registration requests
        ii. Event and Agenda Page with Event Schedule if public
        iii. Download repository and links for public information, if FOUO then a folder in AKO will be used for storage and authentication

iv. Augusta Airport Info
v. Directions Around Augusta with Google Maps API
vi. Local Weather Info
vii. Hotel Information with links and contact information for the following hotels by default:
    1. **Hampton Inn & Suites**
    2. **Holiday Inn, Augusta West**
    3. **Sheraton Augusta Hotel**
    4. **Wingate Hotel**
    5. **DoubleTree**
    6. **Marriot of Augusta**
    7. **Homewood Suites**
    8. **The Partridge Inn**
    9. Fairfield Inn
viii. ONE Primary and Secondary Webmaster and Site POC for general design and problem resolution
ix. Army Policy Links, Declaimers, 508 Compliance and Notices as Per Army Regulation 25-1

Please fill out the following form located @: https://cac.tke.army.mil/sites/signal/ to request a site.

APPENDIX D

Requesting a Unit Level Page Manager for Official Use websites administration

Development of Conference, Special Needs or Event Websites

SUBJECT: Generic Conference/Event Sites

SUBJECT: KM / GARRISON TEAM WEBSITE DEVELOPMENT SECTION – Unit-Org Level (USER) Page Managers

Customers Responsibility:

1. The Customer should request a Page Manager (PM) appointment Via the SIGCoE TKE SharePoint HELPDESK (link: https://cac.tke.army.mil/sites/signal/) *Please read requirements below for required forms*
2. The Customer assumes the understanding that the Top-Level Administration, sub-development, server environment and domain requirements will be handled by the KM/GARRISON Team on behalf of the requesting unit.
3. The Customer assumes the understanding that all development and web programs and technology coding, uploading/installing of design changes, server environment maintenance and other server issues including other webmaster work will be accomplished by the KM/GARRISON Team's IA certified Webmasters on behalf of the requesting unit.
4. The Unit Level Page Manager will need to obtain the following training and forms.
    a. Fill out the PM request form located on the KM TKE Home Page under Web Resources
        i. Attach the Form to the Support Ticket on the TKE HelpDesk
            1. Ensure to Title the Ticket in lines with your request e.g 442nd Page Manager Appointment
            2. After you issue a ticket, a support representative will be assigned to your ticket, he/she will serve as the liaison with you to accomplish all the required steps
    b. Required Training
        i. Go to https://iatraining.us.army.mil/
        ii. Complete the Following Online Training Modules
            1. Social Networking v1.0
            2. Web Content and OPSEC Certification
            3. Personally Identifiable Information (PII) v1.0
        iii. Once Completed, notify the KM/GARRISON Webmaster Team and we will validate the results through the G-6 Office
5. When all forms and training are complete, the KM Team will schedule an appointment with the new Page Manager to get a hands on demonstration of our products and to ensure basic level understanding of web development. Please note the KM Team does not provide personal web based coding or PM training due to limited office resources, but we strive to ensure mission accomplishment no matter the situation.
6. Page Manager Design /Development Guidelines and Responsibilities
    a. The Page Manager assumes all content meets Army OPSEC requirements (ie. PII Deployment info, FOUO etc.); the KM/GARRISON Webmaster Team will serve as the advising authority.

b. The Page Manager will be required to issue changes though the TKE Help Desk attach changes in .Zip file format via the attach files button on the new ticket; the KM/GARRISON Webmaster Team will serve as the final authority to approve web content i.e. coding Quality Assurance.
c. The Page Manager will ensure that the changes are in lines with the SIGCoE / GARRISON provided templates (Document authority is the SIGCoE and USAG-FG/PAO Branding Guide and Development Guidelines)
d. Any special advanced coding requests are handled on a case by case bases.
e. The Page Manager will ensure the site he/she webpage will be maintained, meet OPSEC and up to date at least quarterly to ensure relevance of information.
    i. A automated update notification and verification system including Update procedures and checklist can be found on the TKE Help Desk Home page under sections, Garrison Website and Social Media Inventory or SIGCoE Website and Social Media Inventory. This list should contain the PM's site with relevant contact and OPSEC/Content inspection dates. and Failure to do maintain the webpage or up to date list may result in suspension of services

Please fill out the following form located @: https://cac.tke.army.mil/sites/signal/ to request a site.

-NOTES PAGE-

Note 1: Management Controls are contained in the policy published by the Office of the Secretary of Defense, titled: Establishing and Maintaining a Publicly Accessible Department Of Defense Web Information Service, 9 January 1998.

Note 2: These elements were pulled directly from the DEPSECDEF memo, Information Vulnerability and the World Wide Web, dated 24 September 1998.

Note 3: Technical data creates a unique challenge to the OPSEC posture of an organization and to National Security as a whole. Certain technical data, when compiled with other unclassified information, may reveal an additional association or relationship that meets the standards for classification under Section 1.8 (e) E.O. 12958.

Note 4: "Tip-off" indicators are pulled directly from AR 530-1, Operations Security (OPSEC) regulation, dated 19 September 2007. Tip-off indicators highlight information that otherwise might pass unnoticed. These are most significant when they warn an adversary of impending activity. This allows an adversary to pay closer attention and to task additional collection assets.

By necessity, this list is generic in nature. There are many other indicators possible for the wide range of military operations and activities. While this list is rather large it may be applied with a greater level of accuracy when placed in the context of a command's ***pre-established*** critical information. This checklist is not a panacea for a complete organizational OPSEC program. If an organization has not invested the effort to analyze its own critical information, then this list may only tend to exacerbate the problem.

Within the context of information assurance, the World Wide Web should not be treated any differently from any other potential vulnerability. Security of information on publicly accessible web sites must be viewed in the context of an organization's overall OPSEC posture.