DMA
DEFENSE MEDIA ACTIVITY

DMA PUBLIC WEB HOSTING

DMA Public Web (DMA-PW) is a world-class enterprise hosting service provider of Web services for DoD organizations. The mission of the DMA-PW program is to provide a fast, secure DoD enterprise-level hosting service consisting of Web hosting using a consolidated content management system (CMS) to provide information sharing and economies of scale for the DoD. Currently, the DMA-PW program supports the flagship websites for DoD (www.defense.gov), Air Force (www.af.mil), Navy (www.navy.mil), Marine Corps (www.marines.mil), Army Corps of Engineers (www.usace.army.mil), Joint Chiefs of Staff (www.jcs.mil), and over 700 military and DoD websites.

DMA-PW provides a wide variety of services for publicly-accessible websites and social media blogs including Web development, Web design, system engineering, network operations, security, training, and site migration. DMA-PW also offers marketing services (e.g., e-mail tools, surveys) and analysis of Website traffic and visitor data to help clients attract more visitors to their Websites. In addition, the program provides technically skilled service desk staff to assist clients during normal business hours and 24/7 emergency on-call support. This program supports the DoD Chief Information Officer (DoD CIO) initiative for enterprise services to greatly reduce unnecessary spending for custom development of Web presences.

The DMA-PW offers a wide variety of safeguards to protect client sites such as state-of-the-art security software, high capacity Web servers, heavy-duty firewalls, superior Internet connections, emergency power sources, backup systems, and experienced technical experts. For example, the program uses a content distribution network (CDN) with transmission control protocol (TCP) acceleration technology to boost Internet performance and provide superior streaming quality on client sites. The CDN network is also comprised of interlinked servers distributed across numerous regions for redundancy and protection against cyberattacks. This CDN architecture enables client sites to have 100 percent global availability, regardless of any network issues and power outages.

Summary of Services

- CMS (Content Management Systems) – Easy-to-use, online web site builder software
- Account Management – Collaboration with client to identify needs and matches services
- Content Migration – Work with client to ensure a seamless transition of website hosts
- Training – Train clients with the knowledge necessary to create high quality websites
- Service Desk – Dedicated support provider (during 0630-1700 CST on weekdays and emergency on-call support for nights/weekends)
- Search Engine Optimization – Increase the number of visitors to client website by boosting their search ranking on web search engines
- Web Analytics – Optimize web usage via measurement, collection, and analysis of data
- System Administration and Security – Maintain/protect web hosting systems
- Software Development – Build/upgrade CMS and individual software tools IAW client needs
- Technology Research – Assess new technologies and trends on the web for client use
- Content Delivery Network – Distribute content around the globe quickly and securely
- Live Streaming Support – Deliver live streaming video for events quickly with the help of DMA production staff or Defense Video and Imagery Distribution System (DVIDS)

CONTENT MANAGEMENT SYSTEMS (CMS)

AFPIMS Websites

DMA-PW offers fast, flexible, and easy-to-use CMS options to clients. The client users can make changes to their Websites anywhere, anytime, and on any browser by simply logging onto their accounts with their DoD/Military CAC. Client Websites hosted by DMA-PW use our simple and yet powerful software AFPIMS (American Forces Public Information Management System) to access CMS. The AFPIMS CMS allows client Websites to create desired content, provides attractive/functional templates that meet government regulations, facilitates standardization with parent organizations, and allows sharing of content (e.g., news, press releases, photos, videos, bios). AFPIMS can also be setup to designate content managers that can approve proposed content from users prior to publication.

It also saves money and time that will be expended due to costly Web development, complexity of customization, and cumbersome Web tools. Any client blog sites hosted within the DoDLive environment operated by DMA-PW will also use our user friendly online, all-inclusive software to update their blog content and choose desired themes and plug-ins. DMA-PW currently provides enterprise search capabilities.

With its dynamic functionality, and significant usability and simplicity, it streamlines the content-management process and enables the branches to deliver richer end-user experiences. AFPIMS allows users to apply creative communication techniques to meet their organization's goals. The AFPIMS can disseminate a large amount of information worldwide in only a few minutes.

DoDLive Blogs

Any new clients requesting their blogs to be hosted by DMA Public Web will be required to use our DoDLive content management system. DoDLive is a WordPress core, browser-enabled content management system (CMS) developed in .php code. We maintain the infrastructure and robust distribution system that meets all DoD standards for information security of your blog presence. See more at https://support.dodlive.mil/ (CAC required).

DMA-PW HOSTING SIGNUP PROCESS

For AFPIMS Websites or DoDLive Blogs

New clients interested in hosting their site(s) with DMA Public Web (DMA-PW) can submit an email request to the Public Web service desk (pubwebhd@defense.gov) and they will receive more details about the process. Clients should indicate in their email subject field if their interest is about a new AFPIMS website or a DoDLive Blog.

POLICY

AFPIMS Websites

The following items are required to ensure 100 percent compliance with DoD Web regulations/ policies and/or ensure complete protection of client websites.

- Client will receive access to the AFPIMS content management system, which allows client to create desired content, provides regulation-compliant attractive/functional templates, facilitates standardization with parent organizations, and allows sharing of content (i.e., no direct external database integration, custom codes, CGI bin scripts, web form collection of personally identifiable information, secure/non-secure files transfer protocol, 3rd party executable code).
- All site content will be fully accessible to the public and not blocked with passwords.
- API integration is acceptable but may require additional funds for complex configurations.
- Support will be offered for only the client-side Java applets (i.e., not server-side). DMA will perform security analysis of code.
- DMA will serve as the authoritative Domain Name System (DNS[1]) controller for OSD and DMA sites. Clients for non-OSD/DMA sites will need their own authoritative DNS controller, who will register their domain and CNAME with the Central Registry.
- DMA will offer HTTPS[2] websites later, since HTTPS provides superior confidentiality, authenticity, and integrity.

DoDLive Blogs

The following items are required to comply with DoD Web regulations and policies.

- DISCLAIMER - Link to the DoDLive Disclaimer Page or a page created within the AFPIMS blog site that includes a comment section and a section for external links.
- PRIVACY POLICY - Link to the DoDLive Privacy Policy Page or a page created within the AFPIMS blog site that includes a comment section and a section for external links.
- AVAILABLE THEMES - Blog sites should be created with the themes supported on DoDLive. Exceptions would include pre-existing conditions, but it is recommended these sites change to an available theme to ensure the site remains compatible with any new versions of WordPress and plugins.
- AVAILABLE PLUGINS - Blog sites should use the WordPress plugins available on DoDLive. However, new plugins can be submitted to the DMA Public Web service desk for review. A new plugin should meet the criterion below:
    - Plugin functionality does not duplicate existing ones (i.e., avoid unnecessary duplication).
    - Plugin can be used by the majority of the blogs (i.e., not useful to maintain long-term if it can only be used by a few blogs).
    - Technical elements of the plugin can be properly integrated into the DoDLive WordPress environment.

NOTES

DNS[1]

The Domain Name System (DNS) is the phone book for the Worldwide Web. The Central Registry keeps a directory of domain names in order to convert them into Internet Protocol (IP) addresses, since computers and mobile devices find websites by their IP addresses (e.g., user types in domain name www.organizationx.mil and the DMA's Akamai content distribution network server finds the IP address 211.168.220.71 and then connects the user to that IP).

After the client website has been migrated/built in AFPIMS, the DMA migration team will provide this DNS entry information to the client, who will then forward it to their authoritative DNS controller. DMA will serve as the authoritative DNS controller for OSD and DMA sites. For those sites, DMA will create the client's domain name and desired alias names (called Canonical Name or CNAME) to help users find the client site on the Internet quickly (e.g., client that owns www.organizationx.mil could create www.location2.organizationx.mil for its geographically separated unit). Clients for non-OSD/DMA sites will need their own authoritative DNS controller, who will register their domain and CNAME with the Central Registry.

HTTPS[2]

In the near future, DMA Public Web hosting will use HTTPS versus HTTP in the site URL.
HTTPS provides superior confidentiality, authenticity, and integrity than HTTP.

- Encrypts almost all information sent between a client and a web service
- Protects visitors from spoofed sites and interference by "middleman"
- Prevents interception, tampering, and modification of the data between visitors and the website. HTTP discourages cyber-attackers by making attacks very difficult and expensive.
- Search engines like Google uses HTTPS to rank search results, so this will help users find client's websites.
- Safe-fail for DNSSEC, since DNSSEC does not ensure the confidentiality or integrity of communication between a client and the destination IP. Furthermore, major web browsers do not even inform the user when DNSSEC validation fails.