Public Affairs Mission

Public Web provides customer organizations with a website content management system and hosting solution referred to as AFPIMS, built with the Public Affairs (PA) mission in mind.

Our online training resources at **https://pwtraining.dma.mil/** will enable the average PA professional to post and share their news articles, releases, press advisories, transcripts, speeches, publications, biographies, contracts, imagery, and videos within AFPIMS. The PA professional will be able to share their content across the over 800 web sites hosted in AFPIMS. The PA professional can also incorporate into their own content the existing content from the other AFPIMS web sites.

Orientation

Public Affairs Mission

Technical and Web Design Perspective

Cybersecurity

Customer Service

Public Web Policy and Constraints

There will be no need for the PA professional to rely on any special software or web services team that could affect their online performance or timeline. The PA professional can simply login via an internet browser with their CAC from any location around the world, office, home, remote assignment and complete their tasks at hand.

AFPIMS sites are designed so the content you see while editing appears as it does when it goes live for public viewers to see. The web site in general, specific pages, or specific areas on a page can be customized with various levels of roles and permissions that establish controlled and standardized publishing workflows for any content to be posted. Example of roles may include site manager, content manager, and content provider. More specific roles can be customized for the needs of the PA community. The example of permissions is a content provider allowed to only upload a news story and a content manager to actually approve it for the live post.

An AFPIMS login URL will be provided to the PA professional. Once logged into the site, the PA professional will have access to edit their sites' content based on their roles and permissions.

AFPIMS integrates a suite of technologies:

- The DVIDS Media Player pulls videos and audio uploaded to the DVIDS site onto your site for viewing by the public.
- YouTube videos can be embedded on your sites as well.
- The social media module in AFPIMS pulls in either Facebook or Twitter feeds or both.
- Standard website technology such as RSS and AddThis are also a part of the software collection that can be incorporated into any web site.

- Urchin Analytics is currently the system used for metrics in AFPIMS to analyze traffic for your web site and provides accurate and easy-to-understand web stats, web traffic statistics and reports on your visitors.
- Akamai content delivery network (CDN) technologies will distribute your website content around the world within a matter of minutes from when a PA professional has posted new content or updated any current content.

Technical and Web Design Perspective

American Forces Public Information Management System (AFPIMS) is a DotNetNuke core, browser-enabled content management system (CMS) developed with Microsoft .NET technology. AFPIMS customers will be provided an AFPIMS CAC-enforced Internet address (URL) to log into their respective AFPIMS web site(s). There is no special software needed to build or rebuild a web site within AFPIMS. AFPIMS is basically a website builder with the following standardized design themes referred to as skins.

SKIN TEMPLATES	WEB SITE EXAMPLES
DoD Skin (Available for all customer organization types to include any of the military services with approval by their chain of command)	- http://www.esd.whs.mil/ - https://www.dma.mil/ - http://www.ndu.edu/ - http://www.dla.mil/ - http://dcmo.defense.gov/ - http://www.southcom.mil/ - http://www.armyupress.army.mil/
Joint Skin (Available for all customer organization types to include any of the military services with approval by their chain of command)	- http://www.usar.army.mil/ - http://www.nationalguard.mil/ - http://www.jbsa.mil/ - http://www.pacom.mil/ - http://www.stratcom.mil/ - http://www.navsea.navy.mil/
Army Skin (Exclusive for the Army)	- http://www.usarcent.army.mil/ - http://www.riley.army.mil/
Army Corps of Engineers Skin (Exclusive for the Army Corps of Engineers)	http://www.usace.army.mil/
Air Force Skin (Exclusive for the Air Force)	http://www.af.mil/
Marine Corps Skin (Exclusive for the Marine Corps)	http://www.marines.mil/

AFPIMS customers have the latitude to adjust a particular theme by customizing the cascading style sheet (CSS) code, but they will be responsible for maintaining such customized code and to fix it if it were to break due to scheduled maintenance, which may include periodic AFPIMS system updates.

AFPIMS makes the process of building web sites and managing content simple and quick **for even the most non-technical users.** The functionality and features of AFPIMS is based on the use of modules. The available modules enable AFPIMS users to create and share website elements such as their news articles, releases, press advisories, transcripts, speeches, publications, biographies, contracts, imagery, and videos.

For a complete list of available modules or any other technical or functional details about AFPIMS please visit our online training resources at **https://pwtraining.dma.mil/**.

Cybersecurity

Public Web maintains the infrastructure and robust distribution system that meets all DoD standards for information security of AFPIMS web sites. Public Web is accredited to host **impact level 2 web sites**, information cleared for public release, as well as some DoD private unclassified information not designated as controlled unclassified information (CUI) or critical mission data, but the information requires some minimal level of access control. **Authorization To Operate (ATO)** under the Low-Low-Low categorization level (**Confidentiality-Low, Integrity-Low, Availability-Low**).

Security objective of **Confidentiality-Low Impact:** The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Security objective of **Integrity-Low Impact:** The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Public Web provides a **Risk Management Framework (RMF) accredited, cloud-based hosting solution** against threat actors. Our hosting solution is in accord with DoD best practices and aligned with forward leaning initiatives articulated by the Secretary of Defense and DoD CIO to move into the cloud, decrease cost, and protect public facing web sites with a trusted leading content delivery network (CDN).

We notify AFPIMS customers and other mission partners whenever serious attacks are attempted, and make log/threat data available to AFPIMS customers upon request.

Public Web embraces modern agile processes to continually improve the code base for AFPIMS. Application security is baked into these processes by self-assessments and contracting with DISA for regular Web Vulnerability Scans (WVS). In addition, our developers are also responsive to findings reported by the public researcher (hacker) community.

Public Web was at the forefront of Secretary of Defense Ash Carter's Force of the Future Initiatives, with the first ever Department of Defense (DoD) bug bounty, "Hack the Pentagon." The successes realized by this effort has led to additional bounties with DoD flagship domains and subdomains.

The Defense Vulnerability Disclosure Program (DVDP) spawned from the bounty effort and is proving to be of tremendous value to the Defense Department. The DVDP is evolving into a program that engages public researchers (hackers) to assess any DoD networked device connected to the public internet.

Customer Service

For new AFPIMS customers, a **migration specialist will be assigned** to provide the customer with guidance and assistance for the **first 120 days** of the actual website build or rebuild within AFPIMS, referred to as AFPIMS migration.

Public Web provides service desk support during normal duty hours between 0700 to 2100 Eastern Standard Time (EST) Monday through Friday, and 0900 to 1700 EST Saturday, and *emergency on-call support after normal duty hours. Emergency on-call support is provided between 1800 EST and 0730 EST. The service desk can be contacted for both during normal duty hours and emergency on-call hours via email at **pubwebhd@defense.gov** and phone at **(301) 222-6600**.

*Note: An emergency situation will need to fulfill the following criterion:

- The web site is completely down and needs to be fixed immediately.
- AFPIMS is completely down and needs to be fixed immediately.
- A security incident (e.g. spillage) has occurred on the web site.

Public Web Policy and Constraints

Public Web does not host the DNS for the AFPIMS customer's public URL such as http://www.customer.mil/. The DNS (Domain Name System) is often referred to as the internet's phone book because it converts easy-to-remember hostnames like http://www.customer.mil/ to IP addresses like 216.58.217.46.

An authoritative DNS server holds the actual DNS records (A, CNAME, PTR, etc.) for a particular domain/ address. When a Web address (URL) is typed into a browser, DNS servers return the IP address of the Web server associated with that name. The DNS converts the URL http://www.customer.mil/ into the IP address 204.0.8.51. Without DNS, you would have to type the series of four numbers and dots into your browser to retrieve the web site, which you actually can do.

If you have an existing web site, then you already have an organization (authoritative DNS server) hosting your DNS. But, if you have a brand new web site that does not exist yet, then you will be responsible for hosting your DNS or finding an organization to host your DNS.

CUSTOMER REQUIREMENTS

- New AFPIMS hosting requests must derive from government/military oversight.
- Customers will use AFPIMS for updating their website content hosted by Public Web.

- The AFPIMS user must have a government common access card (CAC) to access the AFPIMS login page.
- The AFPIMS user must register for AFPIMS online training and complete before they are provided AFPIMS login credentials (username/password) for their new site.
- **Customer organization is responsible for hosting the DNS** for their web domain or subdomain (web site) and registering any new URLs.
    - Air Force organizations may need to register new URLs (af.mil subdomains) with Air Force Public Affairs Agency (afpaa.hq.publicweb@us.af.mil).
    - Customer organizations may need to register any new .mil domains at https://www.nic.mil.
    - Customer organizations may need to register any new .gov domains at https://www.dotgov.gov.

WEB SITE LIMITATIONS

- All site content will be **publicly released and fully accessible to the public**.
    - No password protected or CAC required areas are allowed in AFPIMS web sites.
- **No FOUO or sensitive data** will reside on AFPIMS web sites.
- No direct external database integration.
    - API integration is acceptable but could require additional funds for configuration.
- No custom web code, except for CSS.
- No Common Gateway Interface (*CGI*) Bin Scripts.
- **No Personally Identifiable Information (*PII*)** will reside on AFPIMS web sites. Examples of PII include but are not limited to social security number, driver's license number, birth date, place of birth, and personal telephone numbers.
- **Data collected via web forms** is not stored in AFPIMS databases. Such data can only be transmitted to customer designated email addresses.
- No support for server-side Java applets.
    - Support for client-side Java applets requires security analysis of code.
- No third-party, executable code (*i.e. DLL files, etc.*) will run on the AFPIMS infrastructure.
- **Public Web does not provide DNS hosting support** for AFPIMS customers.