silo
BY AUTHENTIC8

WHITE PAPER

Best practices for implementing the DoD PAI directive

silo
BY AUTHENTIC8

About the DoD PAI directive

The internet has become the world's go-to resource for answers and insights about everything. Yet as the volume of publicly available information (PAI) continues to grow, risks associated with accessing web content are escalating as well.

A random click could infect a user's device and network with malware. Online researchers and investigators face an added risk because browsing activity leaves traceable "digital fingerprints" that could be attributed back to a user and their agency or organization. And a pattern of browsing could attract unwanted attention from malicious sources or reveal aspects of a sensitive mission.

That's why the Department of Defense (DoD) issued a directive for all DoD personnel about *Access to and Use of Publicly Available Information*.

For the DoD, even accessing PAI for non-intelligence activities could introduce risk to the employee, their workstation, networks, and even the agency at large. While the directive outlines DoD policy for PAI collection and internet safety, DoD components are given latitude on how they interpret and implement it. And that, in itself, could present a risk factor.

Successful implementation of the PAI directive relies on ensuring all components and their personnel adopt consistent best practice tradecraft and tools to minimize risk. How can the DoD make it happen? In this white paper, we'll tackle the challenge with a look into why this directive is now more important than ever, the hidden risks of online PAI collection, and strategic approaches for hyper-secure online research.

The growing importance of PAI for DoD missions

DoD components are increasingly tapping into PAI to increase operational agility. As an example, the U.S. Air Force ISR research task force has made it a high priority to exploit PAI to reach "next generation ISR dominance." And the USAF 23rd Intelligence Squadron has been training personnel on best practices as they "integrate PAI into more of their operations and multi-intelligence fusion analysis."

While this focus is predominantly intel-oriented, the vast majority of PAI online could be used for innocuous business reasons, and by any DoD personnel. The inherent risks are there for everyone, which is why the directive is critical for everyone.

According to the directive, all personnel "may access, obtain, and use PAI to plan, inform, enable, execute, and support the full spectrum of DoD missions."

Defining PAI and its uses

So what is PAI? The directive defines it as, "Information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting a place or attending an event that is open to the public."

In DoD terms, PAI is raw, unclassified data, not intelligence. In other words, PAI is not synonymous with OSINT (or open-source intelligence), but interacting with it over the clear, deep or dark web carries many of the same risks.

As defined by the DoD, "OSINT is intelligence that is produced from PAI that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."

A key difference is the context in which PAI is used. For example, a DoD user might be researching seemingly benign public websites while preparing for official travel to a foreign country. The slippery slope is that a series of browsing activities – attributed to a DoD employee – could, collectively, reveal nonpublic travel plans of government officials. As a result, an adversary could leverage this information to their advantage, either tactical (an attack) or strategic (insight into U.S. interests to drive intelligence collection).

That risk underscores the implicit power of the PAI directive. "It elevates and operationalizes the use of PAI for DoD to users outside of traditional intelligence and investigative realms… and defines the importance of leveraging specific tools to access it," notes the Federal News Network.

For starters, the directive advises personnel to adopt PAI tools, defined as "applications or capabilities that mine or derive meaning from PAI data and that acquire, analyze, store, and disseminate PAI." These tools can be valuable assets for increasing efficiency.

Minimizing risk, however, relies on users having greater ability to maintain operational security while accessing PAI – even for non-intelligence purposes. A fundamental best practice is to isolate browsing away from the network, providing "non-attribution" as DoD personnel access the web. Another is to use 'managed attribution' to blend in with the crowd, so none of a user's online activity can be attributed to themselves, their device and network, or their organization.

The hidden risks of accessing PAI

One of the vulnerabilities in many organizations is that users often consider their online identity and browsing activities are safe and secure by using a VPN or private browsing. Similarly, DoD employees may believe their network inherently protects their identity. Or that their general PAI research is no need for security concern.

But the hard reality is that many websites and commercially available browsers have an increasing number of ways to track online activity and attribute it to an organization or individual identity without users realizing it.

The DoD PAI directive states that users can access PAI relevant to their missions through the DoD's non-classified network or other DoD-provided networks "in accordance with the risk management framework." So what if a majority of personnel are conducting PAI collection on non-classified networks?

When their research is not for intel purposes, they might make their own assumptions about whether or not their browsing could put themselves or the agency at risk. As DoD employees, leaving any attribution trace of identity and online activity can have severe repercussions, including:

- **Endanger personnel:** Maintaining anonymity is crucial to both the user and the organization. If bad actors suspect their actions or territories may be under scrutiny, they may retaliate with intelligence dossiers of their own regarding the component and personnel, or other form of counter-measures such as cyberattacks
- **Destroy credibility with misinformation:** Another tactic is to feed false information to online researchers, which can destroy the integrity of a mission. Even at a minimum, it could disrupt workflows and arrangements that erode productivity.
- **Infect devices and networks with malware:** If a user's browsing environment is not isolated from their computer or network, malicious content could execute locally on their machine and potentially infect other assets on the same network.

Understanding how users are tracked online

Even with VPNs or private browsing, there are many insidious ways a user's "digital fingerprint" can be tracked online. Protecting people and systems relies on leaving no trace that links online activity back to a user or their organization. So it's important to understand what's going on behind the scenes.

Far beyond location and IP address, a user's online presence can be identified through browser and device attributes such as device types, OS, software/plugins installed, time zone and language settings. This digital fingerprint becomes even more identifiable by their online behavior, including search terms used, websites visited, browsing patterns, time of use, social media connections and account activity.

As many possible identifiers stack up, users may be substantially more exposed than they think. In more mundane purposes, that data is often used to serve up personalized ads and recommendations. But exposure can be exploited for dark purposes as well. Fraudsters could hack websites to seize identity tracking data, or users might click a link that invisibly installs malware. For DoD organizations, though, broadcasting all internet traffic associated with their agency can be the biggest risk of all.

Minimizing risk with best practices for PAI access

As with any DoD policy, DoD organizations are given wide latitude to implement the PAI directive. A survey of top performing organizations reveals how successful agencies have implemented the PAI policy in a way that reduces risk and maximizes positive mission impact. Most importantly, those efforts have been backed by high-level command emphasis on implementing PAI best practices that protect identities, mission-critical information, and network security.

Every user's work-related PAI access requires the same tradecraft considerations, whether it is conducting research to support business decisions (e.g., market research for cost estimates), mission information (e.g., weather forecast for upcoming training events), or open-source intelligence (e.g., adversary military activities in a given theater).

Effective tradecraft for online research includes two vital capabilities: **cloud isolation** and **managed attribution**. Cloud isolation ensures that web browsing is 100% separated from the user's device and network to eliminate risk from malicious web content, malware, etc. Managed attribution helps shield users by giving them greater control over how their identity and activity is attributed online.

How managed attribution is different

Managed attribution empowers users to dictate what is or is not left behind as a traceable digital footprint. It is not the same as mis- or non-attribution, so we'll clarify the difference:

- **Non-attribution** is when users try to stay anonymous for web browsing. But even a VPN or dedicated network will not provide a fully cloaked environment. Risk is still high because browsers, tracking cookies, websites and search engines collect data on many variables that can expose a user's identity.
- **Misattribution** is about intentionally misleading others about one's machine, making it appear as though your environment is a different platform in a different location. This can have certain strategic uses; however, even with private browsing, it's risky trying to maintain a false online identity. Furthermore, the PAI directive states that "DoD personnel will not use false assertions of identity or organizational affiliation for official purposes to access, acquire, or use PAI without complying with cover policies."
- **Managed attribution** refers to "actions to control how attributable information appears to an observer." In web environments, it enables DoD personnel to minimize risk by customizing attributes of how their identity appears to sites they visit and people they interact with online.They can manipulate their digital fingerprint, such as location, IP address, device, operating system, language, and browser to control what is seen on the other end and blend in with local users.

MANAGED ATTRIBUTION SOLUTION

Defined by the DoD as "Hardware, software, networks, accounts, or other measures acquired and used to control how attributable information appears to an observer."

How isolation and managed attribution minimize risk

Managed attribution delivers all the benefits of misattribution, but in a uniquely tailored and safer way, which does not violate cover the "false assertions" doctrine or require cover plans. To successfully implement the PAI directive, look for a managed attribution service with purpose-built capabilities that enforce tradecraft best practices, including:

- **Isolate online research:** Ensure that both general and investigative PAI browsing is separate from personal browsing. It's key to avoid specific settings, actions and behavior patterns that can be used to identify DoD users. A managed attribution service (such as Silo for Research) enables agency teams to use the same computer every day, but isolate web browsing in a securely anonymized, cloud-based environment.

  The Silo cloud isolation platform ensures web code never reaches the endpoint, keeping devices and networks safe from malware. PAI information can be safely collected, stored, translated and shared through the solution, with a full audit trail.

- **Manipulate online appearance:** Safe PAI browsing enables users to blend in with a customized identity, such as changing their location, time zone and language settings to align with foreign sites they might access. DoD users can also avoid standing out by using that region's popular search engines and social media networks, and conducting searches using terms in the local language.

How one agency is implementing the directive

One DoD component has a successful program that implements the PAI directive in a way that maximizes protection of personnel, while optimizing access and use of PAI to support a variety of missions.

Key to their program was to first educate users on how to minimize risk in PAI research using tradecraft best practices and managed attribution capabilities. Using Silo for Research, a purpose-built managed attribution solution, users across the component can conduct online research with greater security and control of their digital fingerprint.

Using any computer, any network and any location, personnel can browse for PAI in a 100% cloud-isolated environment, fully protected against malware infection. And users effectively safeguard their identity by customizing their digital fingerprint with location-specific and context-specific settings.

Silo's suite of productivity tools also enables the component to automate research tasks, maintain complete audit trails of every online session, and manage oversight with a compliance dashboard.

Read the success story

- **Use disposable browser sessions:** To minimize attribution risk, users should start a fresh session each time they browse. A purpose-built solution clears all cookies and tracking data at the end of each session, erasing any evidence of the user's device and online activity.
- **Automate for efficiency and productivity:** The right managed attribution solution should make it safe and easy to work efficiently, such as scheduling jobs, automatically downloading sites for later research, capturing content in isolation, as well as built-in tools for translation and audit trails that agency teams may need.

It's critical to remember that even browsing for seemingly innocuous PAI (like regional weather) can accumulate into a bigger picture of activity that could attract attention from malicious sources. Implementing a managed attribution service is a powerful – and easy – way to infuse hyper-secure tradecraft best practices into everyday operations across the DoD.

Managed attribution is not about 'going covert' or developing a fake online persona. It is about safeguarding machine and network identifiers as well as activities, so nothing is attributed back to the U.S. government. With the right core capabilities, the DoD can effectively implement the PAI directive with greater security at every level of every component organization.

A robust managed attribution solution can also improve efficiency with built-in workflow tools and automated tasks designed to support tradecraft.

Best practice action plan for a successful PAI program

Beyond minimizing risk, a successful PAI program should also focus on capabilities that increase operational efficiency and ensure governance over tradecraft practices. Consider an action plan that helps bring it all together; for example:

1. **Establish senior advocacy for the PAI program.** Having leadership champion the adoption and use of tradecraft best practices and tools is the best way to get everyone on board.
2. **Define and rollout a risk management program for PAI access** along with centerpiece technology solutions, such as a cloud-based service for isolated browsing and managed attribution. Support a successful launch with training for all agency employees so they understand why the tenents of the program matter, the approved tools and how to use them.
3. **Monitor compliance**, including network-level redirection if opt-in doesn't work. Look for a managed attribution solution that has a monitoring program baked in. In addition to admin controls for limiting or blocking access to certain websites, the system can make it easy for management to audit session logs with a dashboard for compliance oversight.
4. **Automatically notify users who are not following appropriate protocol.** To ensure everyone consistently uses the risk management solution to comply with PAI best practices, the system should monitor usage and send automated alerts to encourage employees to use their managed attribution account.
5. **Generate activity reports.** Automated usage monitoring also helps management track when and how much the solution is being used to identify potential issues or training needs in their organization. For instance, reporting can identify how much PAI browsing is done on local networks vs. using cloud isolation on the managed attribution platform.

Optimizing risk management with managed attribution

Online browsing is increasingly riskier as user and device tracking becomes more sophisticated. Many research tools fall short of what's needed to effectively shield identities and activities from harm. To successfully implement the policies and intent of the PAI directive as emphasized by DoD Command, agency teams need to apply tradecraft best practices consistently. And getting there requires an easy path to adoption and compliance.

Deploying a user-friendly managed attribution solution like Silo for Research across the DoD organization can be the most effective way to maximize results – protecting the identities of all DoD personnel and the integrity of every mission. Silo's systematic approach also ensures that management has a built-in monitoring and compliance regime, with the agility to identify risks and training needs early on for prompt action.

See how managed attribution can make a powerful difference — schedule a demo today.