**DoD Notice and Consent Banner**

**Frequently Asked Questions**

**Alternate Language/Views:**

Q1. We would like to use alternate or additional language in our banner. Can we do that?

A1. No. The whole purpose of the banner change is to standardize across DoD (and ultimately across the US Government) on legally approved language. This means you cannot add Privacy Act Statements, banner summary statements or any other additional language. If you believe your situation is unique and that alternate language is required, you may submit a request for an exception, per the policy memorandum, to the DoD Deputy Chief Information Officer for Cybersecurity (DCIO-CS) for approval. Such requests should be fully justified and routed through Rob Mawhinney ([robert.j.mawhinney.civ@mail.mil](mailto:robert.j.mawhinney.civ@mail.mil)) and Richard Aldrich ([richard.w.aldrich2.ctr@mail.mil](mailto:richard.w.aldrich2.ctr@mail.mil)). See Q18 below for details on how to submit a waiver request.

Q2. Can we amend the language slightly to make it fit on our operating system that only accommodates X characters (where X is something less than 1300)?

A2. No. In such cases, please use banner option B. That option is to be used for all operating systems not accommodating 1300 character banners.

Q3. We use an operating system and it can accommodate 4500 characters (or more). Can we amend the language in the banner to spell out all the abbreviations?

A3. No. In such cases, please use banner option A. That option is to be used for all operating systems that can accommodate banners of 1300 characters or more. Many lawyers were involved in developing these two banners and only those two are approved. Please do not make any changes to either without getting written approval from the DCIO(CS)’s office. Submit requests through the POCs, Rob Mawhinney ([robert.j.mawhinney.civ@mail.mil](mailto:robert.j.mawhinney.civ@mail.mil)) and Richard Aldrich ([richard.w.aldrich2.ctr@mail.mil](mailto:richard.w.aldrich2.ctr@mail.mil)). See Q18 below for details on how to submit a waiver request.

Q4. Our operating system will accommodate a banner of 1300 characters but the viewing window in which it is displayed cuts off the last paragraph if we enter it exactly as it is portrayed in Atch 1 of the DoD Memo. Can we modify it so that it all displays in the viewing window.

A4. Removing the extra lines between the paragraphs and removing the carriage return between the first and second sentences should have no impact on the meaning or efficacy of the banner. Nevertheless, we are attempting to move to automated checks and it is not clear at this time whether they will be able to be configured to accommodate extra or missing carriage returns. Since the policy states that, “The banner is mandatory and deviations are not permitted except as authorized in writing by the Deputy Assistant Secretary of Defense for Information and Identity Assurance,” even human inspectors may find your banner noncompliant, unless you have a waiver. As such, to be safest you should submit a request for waiver. See Q18 below for details on how to submit a waiver request.

Q5. What about Contractor systems? Is there a different banner for such systems?

A5. It depends. If it is a “DoD information system” that is merely being operated by contractors, regardless of actual location, then the standard DoD banner set out in the policy is required. If the contractor is operating a “DoD interest computer system” then use the banner set out at pages 68-69 of the ODAA Process Manual, ver. 3.2 (<https://www.dcsa.mil/Portals/69/documents/odaa/ODAA%20Process%20Manual%20Version%203.2.pdf?ver=2018-11-29-102431-710>). If it is neither and merely a contractor system, then consult with the contractors’ legal staff for guidance on what banner is required, if any.

**Mobile devices:**

Q6. How can we implement the banner on mobile devices?

A6. Follow the instructions set out in the applicable for Apple iOS or Android STIG to ensure it is properly implemented on each specific device.

**Scope Issues:**

Q7. Does the language dealing with “attached devices” mean that any user coming in from their home or business machine and accessing a DoD information system loses their expectation of privacy in their home or business machine?

A7. The intent of the banner is to address US Government information systems, not home or commercial business computers. Nevertheless, experience has shown that sometimes people bring into the government workplace privately-owned thumb drives or other auxiliary storage devices and plug them into US Government information systems. There is even a reported case of a (city) government worker who was fed up with the shared arrangement he was forced to endure with his government computer, so he brought his privately-owned computer from home and plugged it directly into the government network at his workplace. United States v. Barrows, 431 F.3d 1246, (10th Cir. 2007) (held the employee had no reasonable expectation of privacy in the home computer he plugged into the government network). We are taking the position that to the extent one brings devices into the government workplace and connects them *directly* to a government information system, one has sacrificed any expectation of privacy in such device and consents to a search of such device. We did not intend to use the *remote* connection of a privately-owned computer from home to a US government information system as the basis for entering the person's home and searching his/her privately-owned computer, though the employee necessarily loses any expectation of privacy in communications between his home computer and the government information system and consents to the monitoring of such communications. On the other hand, people who telework using a government-owned computer additionally have no reasonable expectation of privacy in the issued computer or the communications. In addition to the banner, this is covered by the user agreement signed by the employee.

Q8. Is the new banner to be posted on DoD websites also?

A8.  It depends on whether your website is publicly accessible or not. The new banner is **not** for use on public web sites. On such sites use the "privacy and security notice" provided at Figure 2 of DoDI 8170.01, which applies to publicly accessible web sites. The new banner **is** required to be displayed on “private DoD electronic messaging services” per para.3.10. b. of DoDI 8170.01, which includes DoD web sites that use security or access controls. For External Official Presences (EOPs), such as Facebook or other social media sites, use the Transparency Banner set out in Figure 3 of DoDI 8170.01

Q9. Do we have to banner coalition networks? Do we have to have users of coalition networks sign user agreements?

A9. To the extent the coalition network is considered a “DoD information system,” the answer is yes, it must be bannered. And yes, its users must sign user agreements, unless you believe requiring a user agreement from each user will raise special concerns (e.g., because it conflicts with other agreements that exist between the US and coalition partners, because it conflicts with a NATO-required banner, or other reason). In such cases, please raise those concerns through your component so that it can evaluate them. If the component CIO’s office agrees a waiver should be requested, have a GS-15 equivalent or higher submit the request to the POCs listed in policy.

To the extent DoD operates a system that other coalition partners merely connect to from their own systems, then one should banner the connection point.

Q10. If some systems can only be accessed by going through another bannered system, must both be bannered?

A10. We do not require redundant bannering, so as long as everyone who accesses information system "B" must pass first through information system "A" and information system "A" is bannered, requiring all who log onto it to click through the DoD banner, then information system "B" need not also be bannered. Some organizations place several different information systems behind a portal. They require all who log onto the portal to click through a banner, so all information systems reachable only through the portal need not be separately bannered. If, however, it is possible to reach any IS remotely, wirelessly or otherwise, without first passing through a bannered IS, then that IS must also be bannered. Thus, virtually all systems would have to be bannered for those who physically access it, but a banner for those who remotely access it will depend on whether or not they must pass through a bannered portal.

Q11. Does the policy apply to “applications”?

A11. No, the DoD Banner/User Agreement policy memorandum only applies to DoD information systems, not applications. Nevertheless, if the information system is configured such that one's first access to it could be through an application, then that application would need to be bannered, or the information system would need to be reconfigured to present a banner prior to accessing any applications.

**User Agreements:**

Q12. Are separate user agreements required for NIPR and SIPR systems?

A12. No, you only need one user agreement per user. CTO 08-008A asks if you have accomplished user agreements for all users of NIPRNet systems and SIPRNet systems. You do have to do it for users of both systems, but only one agreement per user.

Q13. Does DoD plan to issue a standard DoD user agreement on the DD 2875?

A13. No we do not plan to issue a standard DoD user agreement. A user agreement is required by DoDI 8500.01 and NIST 800-53, though the format is flexible. Several DoD components wanted to reserve the right to include items very specific to their component. As such, the Policy Memo only requires the inclusion of the language at Atch 2 within your component's user agreement, but additional non-conflicting language may be added. Since every component’s user agreement may be different depending on what they plan to include in addition to the required language from Atch 2, we do not plan to issue a DoD standard user agreement.

Q14. Can user agreements be digitally signed or do they have to be physically signed?

A14. Either is acceptable. There are many ways digital signatures can be obtained. Perhaps the easiest way is to send the user agreement in a .pdf and have the recipients sign and return it. Another method would be to include the text of the user agreement in an e-mail to your users. Direct users to read the agreement then to cut and

paste the following statement in their digitally signed reply: "By signing and returning this e-mail, I have read and agree to be bound by the terms of the user agreement below." Another organization is apparently providing a hyperlink to a secure website where the user digitally signs the agreement. All that is required is that you capture a valid digital signature relating to the exact language in Atch 2 of the DoD memo, and keep the user agreements on file so that they can be accessed and used at a later time, possibly as evidence in a court case. (Some components are also including additional language that does not conflict with the required language to cover component-specific issues. That is also acceptable.)

**Privacy Act:**

Q15: Does clicking through a DoD banner at a DoD website that hosts Privacy Act protected information (such as DFAS’s MyPay) constitute a waiver of one’s Privacy Act rights?

A15: No. The Department unequivocally confirms that there is no waiver of Privacy Act rights intended or effected by the standard DoD logon banner.

The MyPay system is fully compliant with the Privacy Act, and provides numerous safeguards to ensure only appropriate, authorized, use and disclosure of information contained in the system. The MyPay system also provides a number of specialized notices and additional information to clarify the security and privacy protections covering the system.

The banner provides notice to the user regarding the broad nature and scope of the USG's authorized monitoring of its official USG information systems, and the information stored or transmitted on those systems. However, the banner also clarifies that the use and disclosure of such information is only for "authorized USG purposes." For example, regarding information covered by the Privacy Act, the Government's use and disclosure of that information must be consistent with all Privacy Act and other applicable statutory protections.

In addition, as noted previously, the MyPay system provides several additional user notices to clarify its Privacy Act protections, including the required privacy notice, and additional system privacy information in its Frequently Asked Questions (FAQ) page. The FAQ entry also cites to the applicable Privacy Act System of Records Notice (SORN) for the MyPay system, which was published in the Federal Register and is available online at: http://www.defenselink.mil/privacy/notices/dfas/T7336.shtml. These privacy notices, in conjunction with an objectively reasonable interpretation of the DoD logon banner, clearly conveys to users that the MyPay system is fully compliant with the Privacy Act, and that users are not in any way waiving those protections.

The DoD notice and consent logon banner language has been carefully crafted to balance the important need to provide users with complete and accurate notice regarding the Government's monitoring activities for system security and other authorized purposes, while preserving appropriate legal protections, including users' privacy and civil liberties. The language has been approved by the DoD Office of the General Counsel, and the General Counsels and Judge Advocates General of the Military Departments, and I understand also includes input from the Department of Justice.

**Titles:**

Q16. For the implementation of the new DoD consent banner via GPO, should the message title (LegalNoticeCaption) read as "DOD NOTICE AND CONSENT BANNER"?

A16. The title is relatively inconsequential so you may use the above title if you choose, but it is not mandated. The title of Attachment 1 of the DoD Memo was primarily intended to provide a caption for and reinforce that the banner is both standard and mandatory. The optional use of a title can in no case contravene or modify the language of the banner.

Q17. For our network, we add an asterisk before and after the message title to provide a quick glance assessment of GPO application (e.g., if you saw "United States Department of Defense Warning Statement" then GPOs were not applied to the system vice "\* United States Department of Defense Warning Statement \*" indicated that the system inherited at least the domain GPO security settings). Would there be an issue if we continued to add an asterisk before and after the new message title?

A17. We have no objection to the inclusion of an asterisk in the title field if it aids in your administration of the system. You should be aware that some special characters on some systems may create problems. For instance semi-colons in some fields will be interpreted as an end-of-file character, so the rest of the field will be omitted. If asterisks are safe and aid you, adding one to the beginning and end of the title poses no issue for us. You should not, however, add any additional characters to the banner itself—not at the beginning, end or anywhere in between.

**Waivers:**

Q18. What is required to obtain a waiver to the banner/user agreement policy?

A18. Include the following:

1. Waivers are only evaluated when submitted by components, so first coordinate with your component CIO office to provide them with an opportunity to evaluate the request and determine whether they want to support it or not. If they support it, they must make the submission. It can be done via e-mail or letter. A person in the grade of O-6/GS-15 or higher must either sign the request or be identified as having approved the request as submitted.
2. The request must indicate whether it is for a waiver to the banner language, the required user agreement language or both.
3. It must indicate whether a temporary or permanent waiver is being sought.
4. It must indicate whether the extension request applies to NIPRNet systems/users, SIPRNet systems/users or both.
5. It must include a detailed justification for the waiver.
6. It must explain what will be done to mitigate any vulnerability created by the noncompliance.

**Click-Through Issues:**

Q19. Is it permissible to implement the consent banner via a Windows (or other) pop-up dialog box that permits the user to logon by merely closing the box rather than clicking on the “OK”?

Q19. In virtually all cases, no. The policy explicitly states that

The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating “OK.”

Windows, and virtually every other operating system (OS), provides a means of implementing enforceable click-through banners. (Some mobile OSes do not support click-through banners and so are excepted, along with any other OS that provides no solution.) For Windows and the vast majority of OSes that do provide solutions, clicking on a box indicating “OK” is required. Clicking on the “X” in the corner of the dialog box or otherwise closing the box without clicking on “OK” should be configured to prohibit the user from logging onto the system.