



The *Defense Organizational Climate Survey (DEOCS)* is a tool that provides commanders and other Department of Defense (DoD) leaders with important feedback about the current climate within their unit or organization. The *DEOCS* Portal has several security measures in place to ensure that the identities of *DEOCS* participants are protected. This document provides survey administrators, commanders, and DoD leaders with an overview of the new secure survey login system, help with addressing login issues, and how participants’ information is safeguarded.<sup>1</sup>

## Table of Contents

About the Secure Survey Login.....	1
How the Secure Survey Login Process Works.....	2
How to Troubleshoot Secure Login Issues.....	3
Participant Privacy.....	4
Contacting the <i>DEOCS</i> Help Desk.....	6

## About the Secure Survey Login

The secure survey login is a new process for participants to access the *DEOCS*. This new process allows participants to access the survey by entering their DoD ID, e-mail address, or phone number into a universal *DEOCS* login page, without the need for survey administrators to distribute passcodes. With the implementation of the secure survey login, the *DEOCS* system automatically distributes survey access information straight to participants, if an e-mail address was provided on the roster.<sup>2</sup>

Some of the benefits of the new secure survey login include:

- **Easy Access.** Participants are able to access the survey via a link automatically sent to their e-mail, rather than waiting for survey administrators to send a passcode.
- **Automated Outreach.** Recruitment and reminder e-mails will automatically be sent to all survey participants included on the *DEOCS* roster.
- **Decreased Burden on Survey Administrators.** Survey administrators will no longer be required to distribute the *DEOCS* link to their unit or organization.
- **User Authentication.** Only participants included on that unit’s or organization’s roster will be able to take the survey.
- **Enhanced Data Protection.** Once participants submit their *DEOCS*, they will not be able to take the survey again.

<sup>1</sup> For more information about the roles different personnel take in the *DEOCS*, click [here](#), and under step 1, “Prepare,” click on the document titled “User Roles and the *DEOCS* Process.”

<sup>2</sup> This process was tested from August 2020 to March 2021, and results showed no negative impact on survey response rates or responses to survey questions.

- **Additional Data Analysis Capabilities.** The data can be weighted and compared across units and organizations and over time.

This section will provide survey administrators, commanders, and leaders with more detail about the secure survey login process and how it impacts participants' access to the survey, as well as tips to troubleshoot any issues participants may experience when accessing the survey.

### How the Secure Survey Login Process Works

To access the secure survey login, all *DEOCS* participants with an e-mail provided on the roster are automatically sent an e-mail from the *DEOCS* Portal informing them that their *DEOCS* is available and encouraging their participation. Survey administrators will need to provide the survey link to participants without an e-mail on the roster. *DEOCS* participants will then enter their DoD ID, e-mail, or phone number to access their survey.

**Registering a survey.** To register a *DEOCS*, survey administrators must **upload a roster** containing the name and contact information of all individuals in their unit or organization. This roster will ensure that only the individuals within that unit or organization are eligible to take that unit's/organization's *DEOCS*.<sup>3</sup>

**Inviting participants.** Once the survey field date begins, all individuals included in the roster that have an e-mail listed will **receive an automatic e-mail with the link to their unit's/organization's DEOCS**. While an e-mail is automatically sent, it is still recommended that survey administrators or commanders inform their members that the *DEOCS* is available and encourage their participation through as many communication methods as possible. The link is the same for all units, organizations, and subgroups and can be distributed widely: <https://www.surveysdrc.com/DEOCS>.

- Note: Individuals that do not have an e-mail address listed on the roster will not receive an automated e-mail from the *DEOCS* system.

**Taking the survey.** For participants to take their *DEOCS* survey, there are four main steps that accompany the new secure survey login process.

1. **Match to an active DEOCS registration.** Instead of using a passcode to access the *DEOCS*, participants will enter their DoD ID, e-mail address, or phone number on the survey webpage (<https://www.surveysdrc.com/DEOCS>). The information a participant enters **must match** the information that was provided on the roster during registration (i.e., the DoD ID, e-mail addresses, and/or phone number). If the information participants enter does not match what is listed on the roster, participants will receive an error message.

---

<sup>3</sup> For a further description of the information required to register a *DEOCS*, click [here](#), and under step 1, "Prepare," click the document titled "Preparing to Register a DEOCS."

2. **Confidential match to administrative data.** An additional matching process attempts to match participants to the DoD's master administrative records. If the system is unable to match a participant based on the information they provided in Step 1, they will be prompted to provide their DoD ID on a different screen.
3. **PIN creation.** With the new secure survey login, participants have the option to save their responses and return later to complete their *DEOCS*. Participants will create a PIN during login that will allow them to re-enter their survey if needed. If a participant forgets their PIN, they will **NOT** be able to retrieve it and will not be able to re-enter their survey.
4. **Consent to take the *DEOCS*.** Once the participant matches to the roster, prior to accessing their survey, they must consent to taking the survey. After consenting, the participant can begin the survey.

### How to Troubleshoot Secure Login Issues

Below is a list of issues and solutions for participants who are having issues accessing or re-entering their survey.

- **Ensure individuals enter the correct survey website.** To access the *DEOCS*, participants must visit the following website:  
<https://www.surveysdrc.com/DEOCS>.
  - **Security Barriers:** If participants are accessing the survey within a government or military network, firewalls may block access. If this occurs, ask your local IT support to whitelist the *DEOCS* website listed above. Individuals can also access their *DEOCS* through their personal device, such as a laptop, mobile phone, or tablet.
- **Ensure individuals enter the correct DoD ID, e-mail, or phone number.** Any information that a participant enters must match the information provided by the survey administrator included on the roster. The roster information entered could be any combination of DoD ID, e-mail(s) (DoD e-mail and/or a personal e-mail), and phone number (work or personal). Survey administrators should double-check the roster they uploaded to the Registration Portal and provide guidance to participants on which information to enter.
- **Ensure individuals are entering the correct PIN.** The current *DEOCS* system cannot recover forgotten PINs and participants are not able to create a new one. In the case of a forgotten PIN, any questions answered prior to saving the survey or being timed-out due to inactivity will be submitted when the *DEOCS* closes.
- **Direct individuals to the participant troubleshooting document.**<sup>4</sup>

---

<sup>4</sup> To access the participant help document, click [here](#), and under step 2, "Conduct," click the document titled "DEOCS Participant Support."

## Participant Privacy

The Department of Defense is committed to safeguarding the information of Service members and DoD civilians who take the *DEOCS*. This section outlines the privacy and security standards that the *DEOCS* follows. As discussed above, to access the survey, individuals are asked to enter their e-mail or phone number and may be asked to enter their DoD ID. The *DEOCS* has privacy policies and secure technology in place to protect all personally identifiable information (PII).

### Privacy Policies

- **We only report results for subgroups with five or more participants.** OPA reports results to unit commanders and organization leaders at the overall unit or organization level as well as by certain subgroups, such as those designated by the command and those based on sex, race, ethnicity, or pay grade. The presentation of results for different subgroups enables commanders and leaders to better understand the nuances of their unit's or organization's climate and ensures that no group is overlooked. To protect participants' privacy, commanders and leaders will only receive subgroup reports for closed-ended questions if at least five participants respond. If your survey included multiple subgroups and only one subgroup had fewer than five responses, it will be combined with the reportable subgroup that had the next lowest number of participants. For example, if subgroups included on a *DEOCS* were Administration with three participants, Operations with six participants, and Logistics with nine participants, the Administration subgroup results would be combined with the Operations subgroup results.
- Additionally, for subgroups based on respondent identified demographic characteristics, subgroups are considered in sets (i.e., junior enlisted and senior enlisted). If one subgroup in a set does not have five or more participants, no subgroups in that set are reported. For example, if there are three senior enlisted respondents and nine junior enlisted respondents, neither subgroup is reported.
- **Participants' privacy will be protected in combined reports.**<sup>5</sup> For combined reports, if only one subgroup out of the selected had results that were not reportable for a given factor, demographic category, or question, all results for the given item(s) will not be displayed. This protects the one nonreportable subgroup. For example, nine of the 10 subgroups selected for a combined report have reportable results for *Cohesion*, but one has a not reportable result for *Cohesion*. The combined report must exclude results for *Cohesion*. 10 subgroups are selected for a combined subgroup report. Alternatively, if not

---

<sup>5</sup> For more information on combined reports, click [here](#), and once logged into the DEOCS Portal, click "My Applications," then "Interactive Dashboard." Once there, click "Quick Links" and then "Data Overview" to view the "Data Overview" document.

enough individuals respond initially, a combined report can be created that displays results as long as there are results for five or more participants. All 10 subgroups did not display results for male and female participants because fewer than five males and five females responded to the questions. When combined, more than five males and five females responded to the questions, so results for male and female participants are included in the demographic category charts.

- **Our practices meet the highest standards of records management and privacy.** The *DEOCS* team has decades of experience collecting and storing sensitive personnel data on behalf of the DoD. Our practices are compliant with all DoD policies regarding information collection.
- **Confidentiality.** Survey answers are confidential to the extent that the law permits. Under state and federal law, certain circumstances may require us to break confidentiality. For example, if a participant indicates a direct threat to harm themselves or others within their responses.
- **Survey administrators, commanders, and leaders cannot view who has completed a survey.** Your responses are combined with the responses of everyone in your unit or organization to produce results of the entire group or subgroup. Consistent with industry-standard practices, personally identifying information from *DEOCS* rosters (e.g., e-mail address) is used within the survey system for outreach purposes and identity verification purposes at survey login (to ensure the right people are taking the survey, and each person can only take the survey once). This information is not included in the reports we provide to commanders, leaders, or anyone else in your unit or organization.
- **OPA never stores PII in the same file with *DEOCS* responses.** Identifying information is always stored separately in a tightly restricted file.
- **We only publish statistics.** OPA does not identify individuals in the reports we provide to survey administrators, commanders, or leaders.

### Website Privacy

- **Neither the DoD nor its survey operations contractor, Data Recognition Corporation (DRC), will collect participant PII when they visit the *DEOCS* website unless participants choose to provide it.**
- **Our system does not enable “cookies.”** Cookies are files placed on a user’s computer’s hard drive to monitor their use of the website and web.

- **The DEOCS does collect non-PII from survey participants' visits.** This information is used to assist the DoD and our survey team in improving the website and overall performance of our web-based surveys. The data collected are listed below:
  - The Internet Protocol (IP) address for the computer or device being used to take the survey (for example, www.verizon.com, www.comcast.com, 122.3.55.34). Depending on the internet service provider, IP addresses may identify the computer or they identify no more than the internet service provider (such as Verizon or Comcast).
  - The device that is used to access the survey (e.g., PC, tablet, or mobile phone).
  - The type and version of the browser and operating system that are used to access the DEOCS website.
  - The date and time that this website is accessed.
  - The number of bytes sent and received.
  - The pages visited.

### Secure Technology

- Working with top industry partners and contractors we have designed our systems with overlapping **layers of security** to protect participants' information from cyber-attack. All systems comply with NIST RMF security standards, as required by the DoD.
- Response data and PII is **encrypted** during data collection and then stored in a **secure network** isolated by firewalls and other security measures.
- We actively monitor all digital traffic and inspect our IT systems to make sure participants' information stays secure.
- To ensure that all survey responses are secure while being transmitted over the internet, the web survey application uses Secure Socket Layers (SSL) with **256-bit encryption**; when participants access the web survey, they will see the "padlock" icon displayed in their web browser.

### Contacting the DEOCS Help Desk

If you have questions or have any problems requesting a DEOCS, please contact our help desk at:

- [DEOCS@datarecognitioncorp.com](mailto:DEOCS@datarecognitioncorp.com)
- 1-833-867-5674

If you have questions about DEOCS content, purpose, or participant privacy, please contact the DEOCS Help Desk at:

- [DEOCS\\_Support@forsmarsh.com](mailto:DEOCS_Support@forsmarsh.com)