

Thank you for requesting a JACCIS account. Below are the instructions for requesting a JACCIS account. If you have any questions contact the DNDO JAC at 1-866-789-8304 or email at [dndo.jac2@hq.dhs.gov](mailto:dndo.jac2@hq.dhs.gov).

### **Applying for an account**

- Fill out the Access Request Form (ARF) selecting S&L Admin, S&L User, or Federal Read Only as the "user type" and the Rules of Behavior (ROB) below and email them to [dndo.jac2@hq.dhs.gov](mailto:dndo.jac2@hq.dhs.gov). Both forms have the ability to create digital signatures in Adobe. The final two pages list the instructions for creating a digital signature.
- A sponsor (leave blank) located here at DNDO will complete your form and provide you an account.
- If a S&L user account, this is your only step

### **S&L Admins creating S&L Users**

- If an Admin account is requested, this will allow you to create other new users within your state.
- Have your other S&L users (must be in the same state as you) fill out and digitally sign both the ARF as S&L Users and ROB Forms and have them sent to you.
- On their ARF fill out and sign as their sponsor then send both completed forms to [JACSEC@dhs.gov](mailto:JACSEC@dhs.gov) (note: this is for tracking purposes only, no further approval is needed)
- Log in with your S&L Admin account.
- Scroll over the Admin tab of the website and select user management.
- Search for the user's last name to ensure they do not already have an account.
- Complete the mandatory fields of Last name, email (their login), security role (S/L User), passphrase and new password. Ensure there is a check next to "Active:" and "User enabled:". Then Click create new user. All notifications will go to their login so please use an active email account
- Provide the new user with the JACCIS URL: <https://jaccis.dhs.gov/JACCIS>, their user name (email) and password that you created.
- Inform user that they can change their password, passphrase, and input their default information for alarm adjudication (ie equipment and location) under their My Profile. This information will auto populate a new alarm allowing for quicker adjudication times.

If you have any questions feel free to email [DNDO.JAC2@hq.dhs.gov](mailto:DNDO.JAC2@hq.dhs.gov). Once logged in, the help tab is very useful in understanding how to use JACCIS. It loads a PDF file with bookmarks on the left. The best way to use it is click on the "How Do I" bookmark. This takes you to a list of tasks broken up by user type.

# Joint Analysis Center Collaborative Information System

## Access Account Request Form v2d

### Location

<input type="checkbox"/> DNDO	<input type="checkbox"/> Lab	<input type="checkbox"/> State & Local	<input type="checkbox"/> Other _____
-------------------------------	------------------------------	--	--------------------------------------

### Select User type

*\*The Review and Approval section below must be completed if requesting JAC ADMIN, SYS ADMIN, CTOS ADMIN, LSS ADMIN or S&L ADMIN privileges.*

### Requester

Name:	First	MI	Last
Organization:			
Title:			
Email:		Phone:	
Reason for access:			

\_\_\_\_\_  
Requester Signature:

\_\_\_\_\_  
Date:

### Sponsor

Name:	First	MI	Last		
Organization:					
JACCIS Role	<input type="checkbox"/> SYS ADMIN	<input type="checkbox"/> S&L Admin	<input type="checkbox"/> ISSM	<input type="checkbox"/> JWO ADMIN	<input type="checkbox"/> list other _____
Email:		Phone:			
Remarks:	<input type="checkbox"/> U.S. Citizenship verified				

\_\_\_\_\_  
Sponsor Signature:

\_\_\_\_\_  
Date:

**Sponsor Notes:** In remarks section, describe how the user was identified (e.g. military id, driver's license, etc.) and how U.S. Citizenship was verified. The sponsor must have a current JACCIS account: email copy of completed form to [jacsec@dhs.gov](mailto:jacsec@dhs.gov), provide original signed copy to ISSO.

**Review and Approval** Completed by JAC (this section must be completed if requesting "JAC Admin", "Sys Admin" or "S&L Admin" privileges as approval is required from the Authorizing Official, System Owner, or Program Manager)

<b>Name:</b>	<b>First</b>	<b>MI</b>	<b>Last</b>
<b>Organization:</b>			
	<input type="checkbox"/> <b>Authorizing Official</b>	<input type="checkbox"/> <b>System Owner</b>	<input type="checkbox"/> <b>Program Manager</b>
<b>Email:</b>			<b>Phone:</b>
<b>Remarks:</b>			

\_\_\_\_\_  
**Approval Signature:**

\_\_\_\_\_  
**Date:**

# Joint Analysis Collaboration Center Information System (JACCIS)

## Rules of Behavior

Version 3a

Prepared for

**Department of Homeland Security  
Domestic Nuclear Detection Office (DNDO)**



**8 November 2011**

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "**FOR OFFICIAL USE ONLY**", OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS MUST BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, MUST BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS, AND UNAUTHORIZED DISCLOSURE.

## 1.0 Rules of Behavior

Rules of Behavior (ROB) regarding the access of Department of Homeland Security (DHS) systems and the use of its IT resources are a vital part of the DHS IT Security Program. ROB that are understood and followed help ensure the security of systems and the confidentiality, integrity, and availability of sensitive information.

ROB inform users of their responsibilities and let them know they will be held accountable for their actions while they are accessing DHS systems and using DHS IT resources capable of accessing, storing, receiving, or transmitting sensitive information.

DHS 4300A Appendix G authorizes DNDO / JACCIS to tailor the General Rules of Behavior for DNDO as well for System Specific Roles of Behavior as indicated below. In addition, DNDO is responsible for developing JACCIS ROB and having users read and sign them.

These rules of behavior are consistent with IT security policy and procedures within DHS Management Directive 140-1 (Information Technology Systems Security), DHS Sensitive Systems Policy Directive 4300A, and the DHS 4300A Sensitive Systems Handbook.

## 2.0 General Rules of Behavior

DHS office equipment includes DHS owned workstations, laptops, or PEDs.

- ✓ *I understand that I will be held accountable for my actions while accessing and using DHS systems and IT resources.*
- ✓ *I understand that I have no expectation of privacy while using any DHS equipment and services, including internet and email.*
- ✓ *I understand that I may be monitored and that disciplinary actions may result from any violations. I consent to monitoring.*
- ✓ *I will not attempt to access systems that I have not been authorized to access.*
- ✓ *I will not install unauthorized or personally owned software on DHS office equipment.*
- ✓ *I will not connect non-DHS office equipment to the DHS network.*
- ✓ *I will not attempt to bypass access control measures for systems I have been authorized to access.*
- ✓ *I will not share passwords or access numbers with anyone, including system administrators.*
- ✓ *I will promptly change a password if I suspect that it has been compromised or disclosed.*
- ✓ *I will protect sensitive information from disclosure to unauthorized persons or groups.*
- ✓ *I will log off or lock my workstation or laptop computer, or I will use a password-protected screensaver, whenever I step away from my work area.*
- ✓ *I will log off when I leave for the day.*
- ✓ *I understand that DHS office equipment is to be used for official use, with only limited personal use allowed as described in DHS policy.*

- ✓ *I understand that the viewing of pornographic or other offensive or graphic content is strictly prohibited on DHS office equipment.*
- ✓ *I understand that the use of webmail or other personal email accounts is prohibited on DHS office equipment.*
- ✓ *I agree to comply with all software copyrights and licenses.*
- ✓ *When away from my primary workplace, I will follow security practices that are the same as or equivalent to those required of me at my primary workplace.*
- ✓ *I will physically protect any DHS office equipment and data in my possession when away from my primary workplace.*
- ✓ *I will keep antivirus and firewall software on the laptop active and up-to-date.*
- ✓ *I understand and will comply with the requirement that sensitive information transmitted from or stored on laptops or wireless devices must be encrypted using approved encryption methods.*
- ✓ *I will promptly report suspected IT security incidents.*
- ✓ *I will not access DHS Systems until I have signed the Rules of Behavior.*

### **3.0 JACCIS Specific Rules of Behavior**

- ✓ *I understand that U.S. Citizenship is required to access JACCIS.*
- ✓ *I understand that there is no expectation of privacy when using JACCIS.*
- ✓ *I understand that JACCIS is not certified to process classified national security information.*
- ✓ *I understand that DHS may conduct JACCIS monitoring activities without further notice.*
- ✓ *I understand that JACCIS is not certified to process, store, or transmit Sensitive PII data.*
- ✓ *I understand that JACCIS contains PII and I will safeguard such data accordingly.*
- ✓ *I understand that I may not extract data from JACCIS for purposes not related to JAC operations.*
- ✓ *I understand that hyperlinks sent to the JAC via email may contain links to fraudulent (non-JACCIS) sites (phishing attacks), and will not enter JACCIS password unless certain I am at the authentic JACCIS web site (<https://jaccis.dhs.gov>).*
- ✓ *If my JACCIS user role includes “S&L Admin” privileges, I will immediately notify DHS DNDO when users no longer have a need to access the system due to the user’s separation, transfer, or termination (etc).*
- ✓ *If my JACCIS user role includes “SYS Admin”, “JWO Admin”, or “S&L Admin” privileges, I will not create any JACCIS account without ensuring the following tasks are completed on behalf of the user requesting access:*
  1. *Verification of U.S. Citizenship.*
  2. *Approval of completed JACCIS Account Request Form (ARF).*
  3. *Signed copy of the JACCIS Rules of Behavior.*

## Acknowledgement Statement

---

I acknowledge that I have read the rules of behavior, I understand them, and I will comply with them. I understand that failure to comply with these rules could result in verbal or written warning, removal of system access, re-assignment to other duties, criminal or civil prosecution, or termination.

---

**DHS Component**

---

**Location**

---

**User Name**

---

**Email Address**

---

**Phone Number**

---

**Supervisor Name**

---

**Email Address**

---

**Phone Number**

---

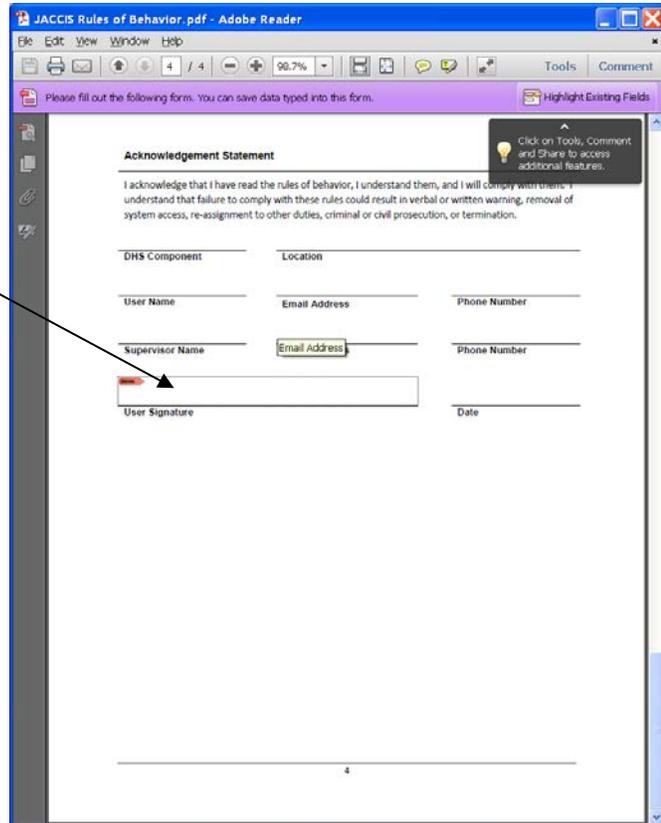
**User Signature**

---

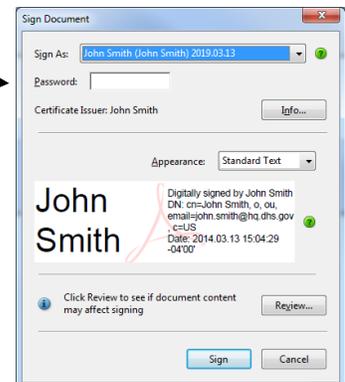
**Date**

## How to create an Adobe Digital signature

1. Click on the location where a signature is requested

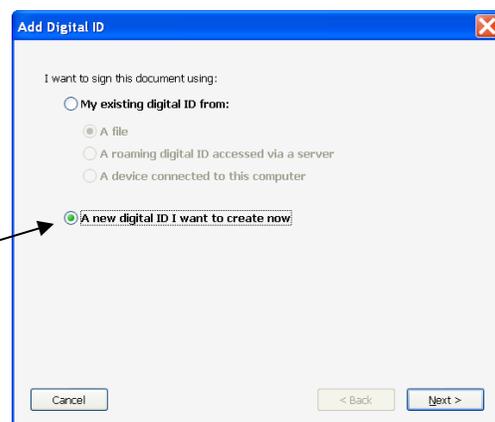


2. If you have already created a digital ID just enter your password



3. If you have a saved file that it did not immediately recognize, load by selecting "My existing digital ID and File. You will then browse to where it is located.

4. If not create a new digital ID



5. Select a new PKCS#12 digital ID File and click next

Where would you like to store your self-signed digital ID?

**New PKCS#12 digital ID file**

Creates a new password-protected digital ID file that uses the standard PKCS#12 format. This common digital ID file format is supported by most security software applications, including major web browsers. PKCS#12 files have a .pfx or .p12 file extension.

**Windows Certificate Store**

Your digital ID will be stored in the Windows Certificate Store where it will also be available to other Windows applications. The digital ID will be protected by your Windows login.

Cancel < Back Next >

6. Fill out the form with your name, organizational information, email address. The Rest should remain as below. Click next.

Enter your identity information to be used when generating the self-signed certificate.

Name (e.g. John Smith):

Organizational Unit:

Organization Name:

Email Address:

Country/Region: US - UNITED STATES

Enable Unicode Support

Key Algorithm: 1024-bit RSA

Use digital ID for: Digital Signatures and Data Encryption

Cancel < Back Next >

7. Select where you would like to save your ID for future use, create a password and click finish.

Enter a file location and password for your new digital ID file. You will need the password when you use the digital ID to sign or decrypt documents. You should make a note of the file location so that you can copy this file for backup or other purposes. You can later change options for this file using the Security Settings dialog.

File Name:

D:\Documents and Settings\nathaniel.evans\Application Data\Adobe\A

Password:

Not Rated

Confirm Password:

Cancel < Back Finish