COMMON SECURITY WARNINGS & SITE ACCESS ERRORS

Are you getting a site certificate error when trying to access this web site? This web site uses SSL protection to help secure our content. Access to these areas require that a site security certificate is loaded into your browser. There are two ways to avoid site certificate error messages:

1. Add an Exception (Mozilla Firefox only) / Create a Trusted Site (IE only).
2. Import a DoD Root CA 3 Certificate (preferred).

While adding an exception is the faster, easier process, you might have to repeat the process for multiple protected DoD web sites. Importing the DoD Root CA 3 Certificate will take about 2 minutes, but it is the more thorough solution. You should only have to import it once per browser. You may see some other messages, usually alerts, rather than error messages, even when everything is installed correctly.

3. Other Common Error Messages

1. Add Exception/Create Trusted Site

- **Add an Exception (Mozilla Firefox only)**
  If you receive a Secure Connection Failed message in Mozilla Firefox, you have the option of simply adding an Exception, thereby making it a Trusted Site. To do so, complete the following steps:
  1. On the error window, click ***Or you can add an exception***; the page reloads.
  2. Click ***Add Exception***; the ***Add Security Exception*** window opens.
  3. Click ***Get Certificate****;* the window reloads.
  4. Check the ***Permanently store this exception*** box; then click ***Confirm Security Exception***.

- **Create a Trusted Site (IE only)**
  In IE, you may receive an error message stating that there is a problem with this website's security certificate. You have the option of making it this site a Trusted Site. To do so, complete the following steps:
  1. Go to ***Tools > Internet Options***.
  2. Select the ***Security*** tab.
  3. Click ***Trusted Sites***.
  4. To create a Trusted Site, click ***Sites***; the ***Trusted Sites*** window opens.
  5. Enter the URL of the desired site.
  6. Click ***Add***. The site is listed in the ***Trusted Sites*** box.
  7. Check ***Require server verification (https:) for all sites in this zone***.

2. Import a DoD Root CA 3 Certificate

- IAD web site users will need to have the current DoD Root and Intermediate Certificate Authorities CA) loaded into their browsers to avoid receiving untrusted web site notifications. Current DoD root and intermediate CA can be downloaded and installed using the InstallRoot 5.0.1 NIPR Windows Installer from the Information Assurance Support Environment (IASE) site under the Trust Store tab. A user guide for InstallRoot 5.0 is available on the same page.

3. Other Common Error Messages

- **Switching from HTTP to HTTPS Pages with IE**
  If you enter the site URL starting with http, instead of https, or if the page you're coming from had a URL starting with http and the link to the secure site was coded with a relative link, you may see a security warning. Select ***Yes*** to proceed.

- **Accessing a Protected Site with IE**
  When opening the site in IE, you may be asked to confirm that it's OK to go to a secure site. You may then have to identify your certificate. You may also encounter a series of prompts. On the first screen, select ***Continue to this website***. On the following screens, select ***Yes*** or ***OK*** as prompted