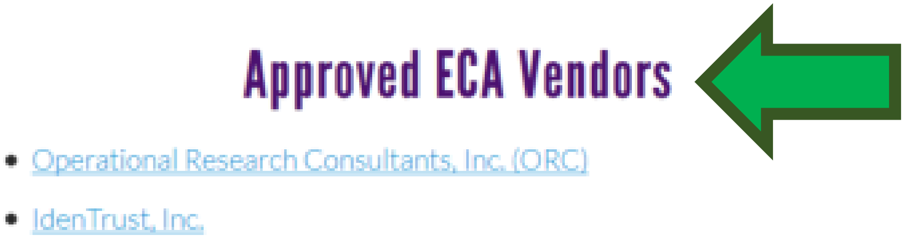
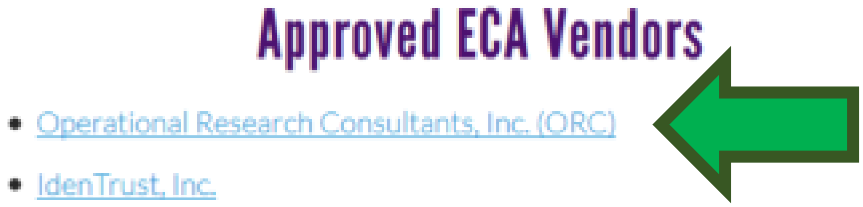
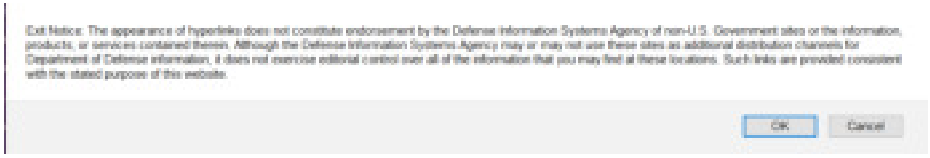
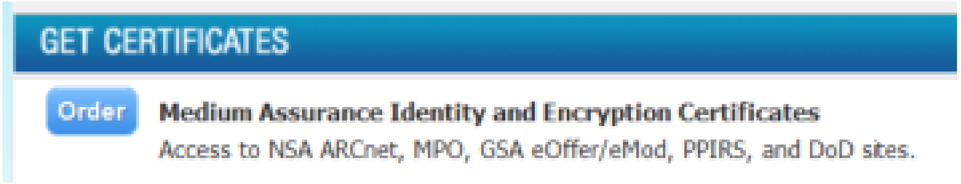
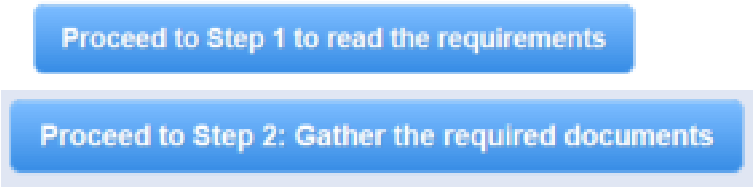
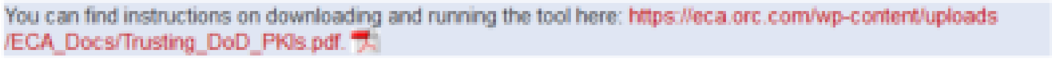
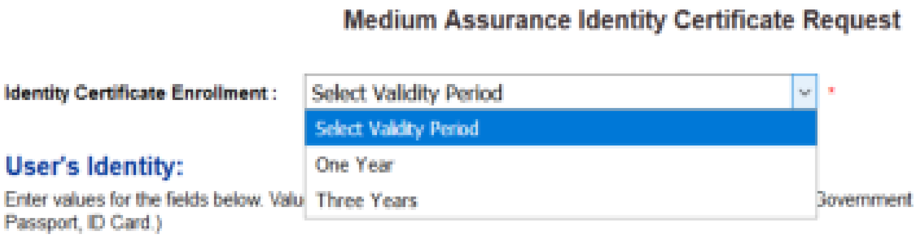
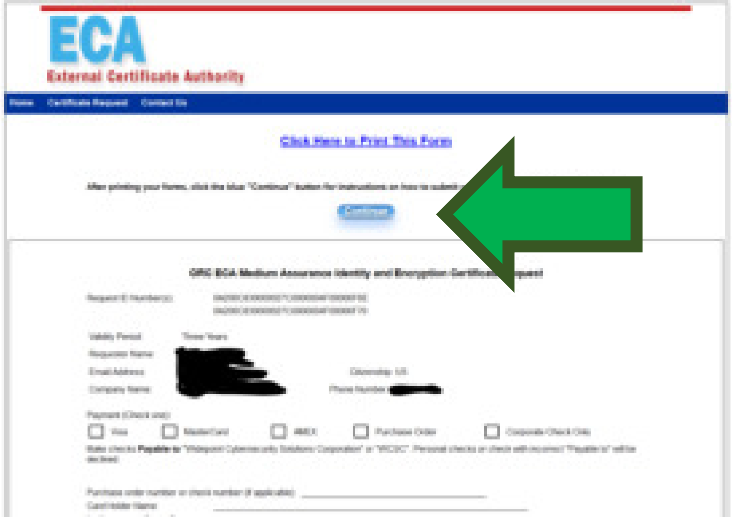
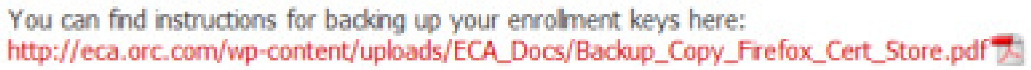
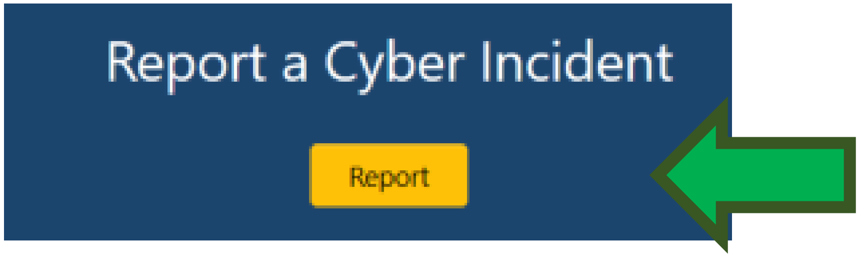
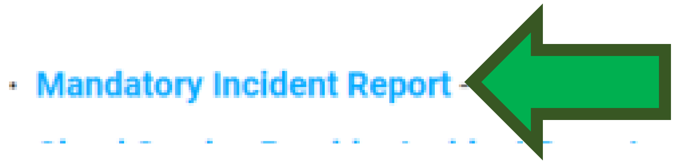
Step	Description	Screen Shots/Notes
1.	Choose a person who will apply for the ECA certificate, and a machine the cert will be installed upon	The ECA certificate will be tied to a particular user in the organization. This user will be responsible for reporting cybersecurity incidents to the DoD. The ECA certificate can be: A. Installed in a Windows machine to be available to IE, Firefox, or Chrome browsers B. Installed on a smart card or USB dongle, and portable to other machines Option A (Medium Assurance Certificate) is the simplest and cheapest method, and is the option covered in these instructions.
2.	Choose whether you want to order a 1 year or 3 year certificate.	As of May 2019, the prices are as follows: • One Year: $109 • Three Year: $245-$249 You aren't required to get one or the other; if you plan on processing CUI for more than one year, the three-year cert is recommended.
3.	NOTE: Perform the rest of these steps on the machine you plan on installing the certificates on. Use the Firefox web browser to perform the steps.	As stated on the ECA request site: Remember that when importing your certificate, you must use the same computer, network profile (log on), and web browser that you used to make the request. Please refrain from all updates of browser and operating system until your certificates have been successfully imported.
4.	Go to the DISA ECA site: https://public.cyber.mil/eca/ . At the bottom of the page, see the **Approved ECA Vendors links**	 Approved ECA Vendors • Operational Research Consultants, Inc. (ORC) • IdenTrust, Inc.

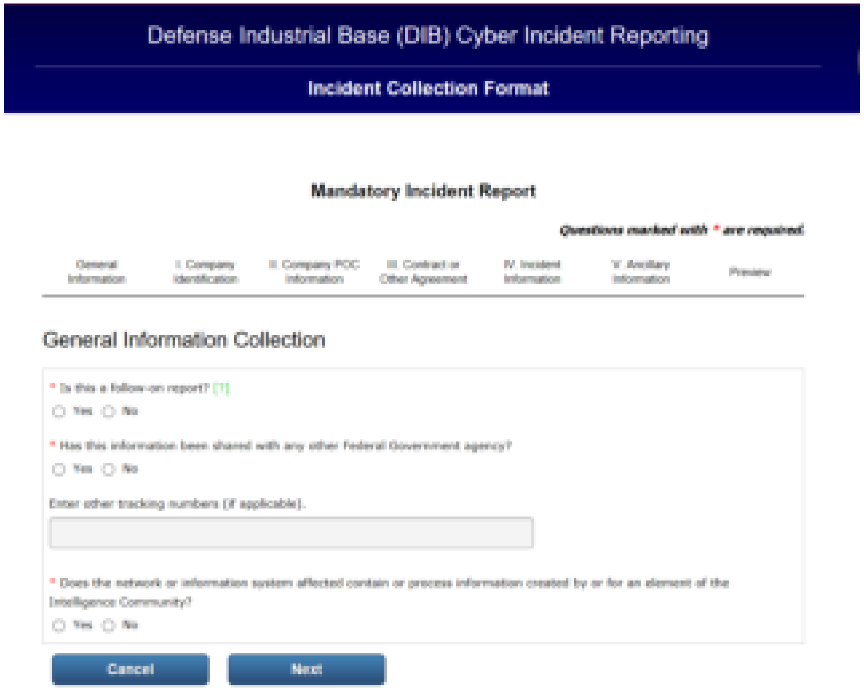
5.	Click the **ORC** link If choosing the IdenTrust website, go to Step #17.	 Approved ECA Vendors - Operational Research Consultants, Inc. (ORC) - IdenTrust, Inc.
6.	Click **OK** at the Exit Notice	 Exit Notice: The appearance of hyperlinks does not constitute endorsement by the Defense Information Systems Agency of non-U.S. Government sites or the information, products, or services contained therein. Although the Defense Information Systems Agency may or may not use these sites as additional distribution channels for Department of Defense information, it does not exercise editorial control over all of the information that you may find at these locations. Such links are provided consistent with the stated purpose of this website.
7.	In the middle of the page, click the **Order** button for Medium Assurance Identity and Encryption Certificates	 GET CERTIFICATES **Medium Assurance Identity and Encryption Certificates** Access to NSA ARCnet, MPO, GSA eOffer/eMod, PPIRS, and DoD sites.

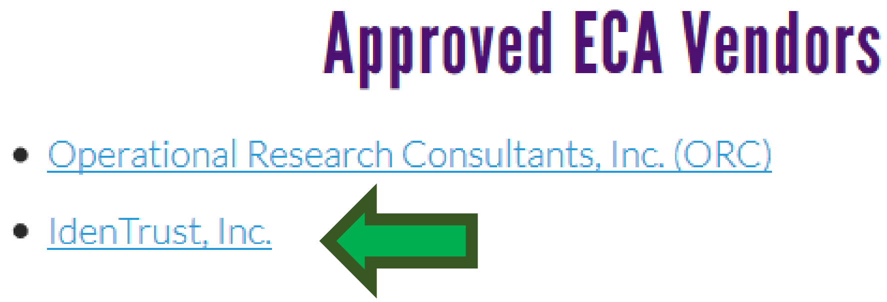
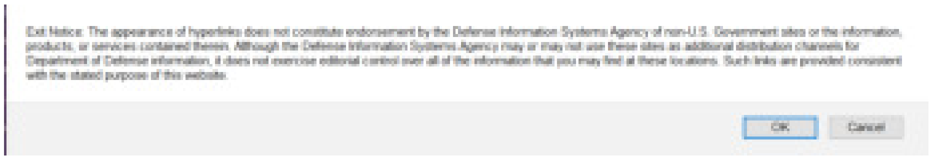
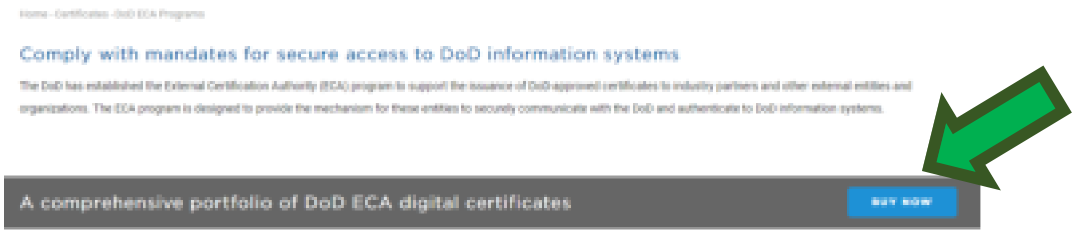
8.	Click the **Proceed to Step #…** buttons to work your way through the application process. When you get to **Step 3: Trust CAs**, follow the link for the PDF with instructions on running the Install Root tool. (You may want to right-click this link and choose “Open link in new tab” because this website isn’t great with returning you to the guide through pages). Run this tool on the computer you plan on installing the certificate on.	 Proceed to Step 1 to read the requirements Proceed to Step 2: Gather the required documents  You can find instructions on downloading and running the tool here: https://eca.orc.com/wp-content/uploads/ECA_Docs/Trusting_DoD_PKIs.pdf.

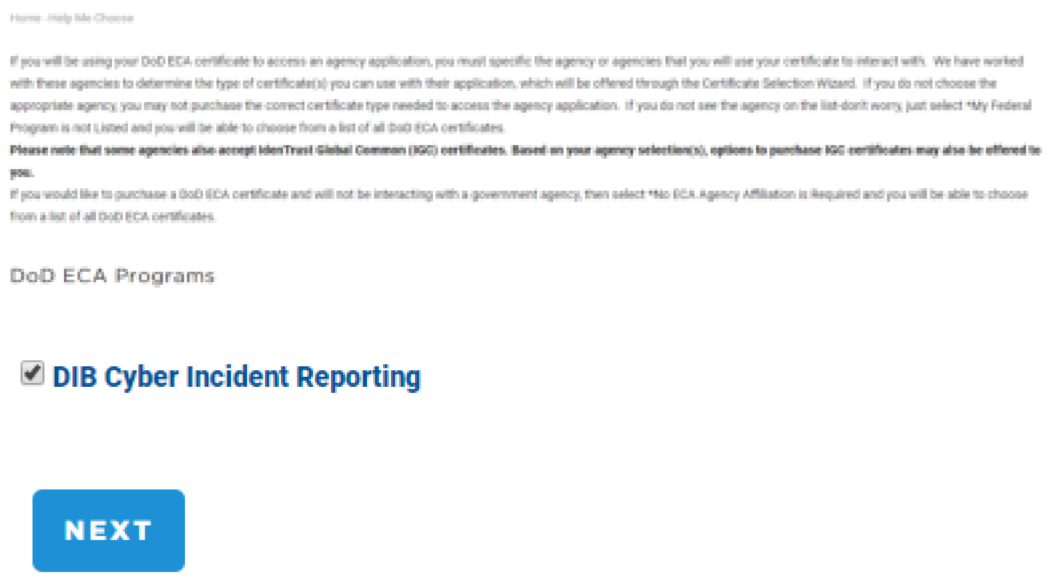
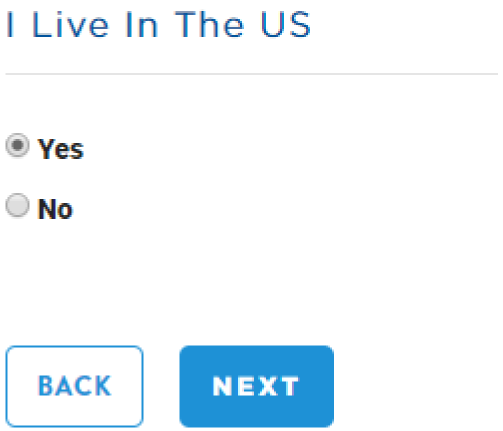
9.	On **Step 4: Request Your Certificate** the walk through will take you to the request page. Choose the length of certificate you wish to obtain. Enter the information for the person in the organization you want the certificate to be associated with. Keep in mind, this person will need to visit the notary to have the forms. Click Submit and then confirm submission.	 Medium Assurance Identity Certificate Request Identity Certificate Enrollment : Select Validity Period * Select Validity Period One Year Three Years User's Identity: Enter values for the fields below. Valu Government Passport, ID Card.)
10.	Once you submit the request, forms will be generated that you can print and have notarized. You'll need to provide payment information on these forms as well. NOTE: Don't photocopy or scan the forms. They, with copies of documentation and notary seal, need to be snail-mailed into the ECA office. Once you have the forms downloaded, click **Continue**.	 ECA External Certificate Authority Home Certificate Request Contact Us Click Here to Print This Form After printing your forms, click the blue "Continue" button for instructions on how to submit Continue ORC ECA Medium Assurance Identity and Encryption Certifica quest Request ID Number(s): [illegible] [illegible] Validity Period: Three Years Requester Name: [redacted] Email Address: Company Name: Citizenship: US Phone Number: [redacted] Payment (Check one) □ Visa □ MasterCard □ AMEX □ Purchase Order □ Corporate Check Only Make checks **Payable to** "Widepoint Cybersecurity Solutions Corporation" or "WCSC". Personal checks or check with incorrect "Payable to" will be declined. Purchase order number or check number (if applicable): ____ Card Holder Name: ____

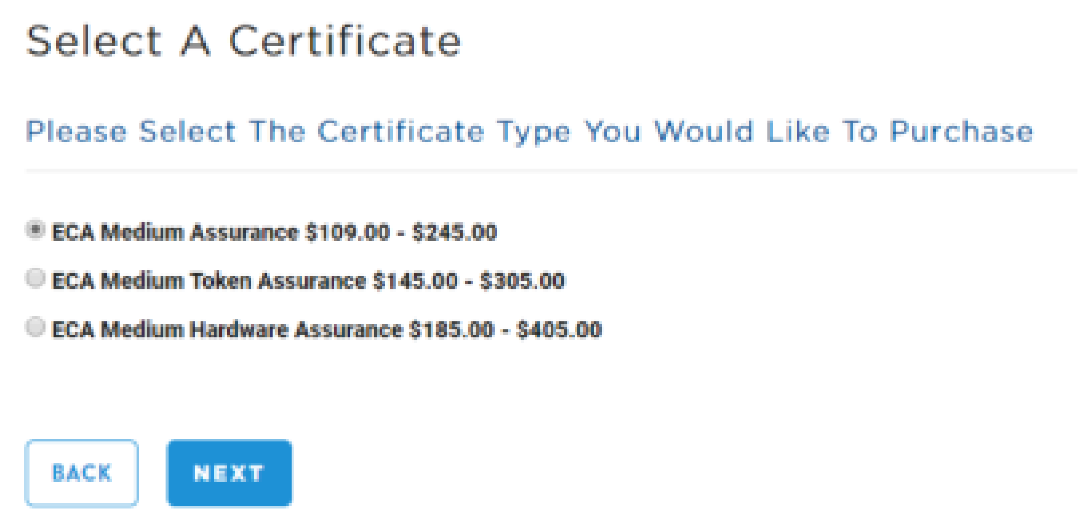
11.	At **Step 5: Back Up Keys**, make sure you follow the instructions in the link to the PDF.	 You can find instructions for backing up your enrollment keys here: http://eca.orc.com/wp-content/uploads/ECA_Docs/Backup_Copy_Firefox_Cert_Store.pdf
12.	Follow the instructions on **Step 6: Notarize & Mail Request**	Per the website: We will process your request within 3-5 business days of its arrival at our Fairfax, Virginia office. Within that time frame, you will receive an email that either: • Informs you of any problems with the request and explains how to rectify the problems; OR • Informs you that your certificate has been issued and provides complete instructions on how to import, test, and create a backup copy of your certificate.

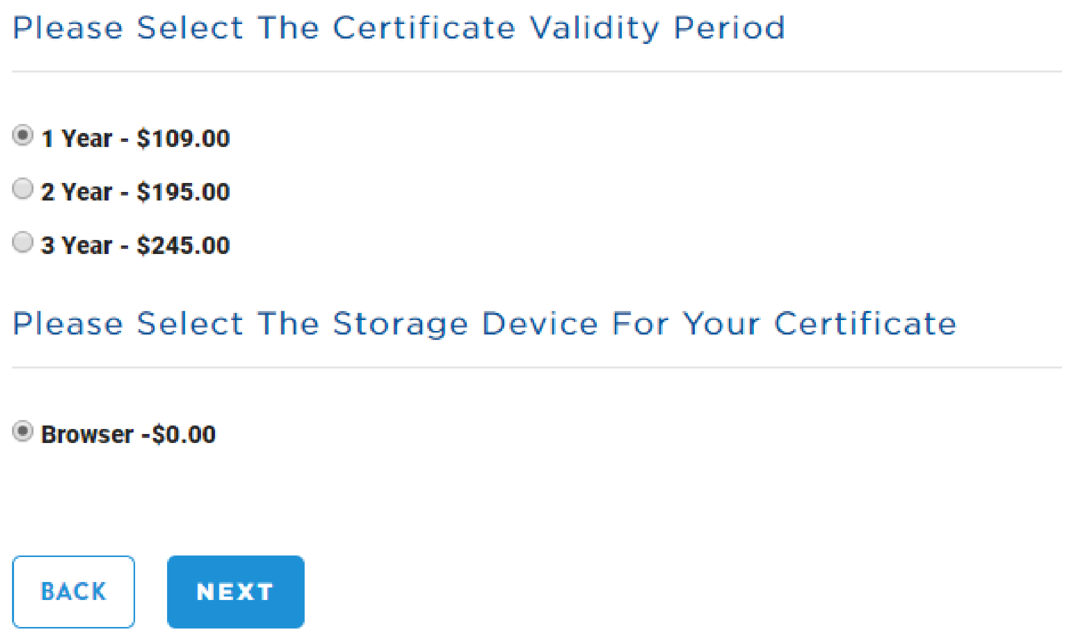
13.	Once you receive the certificates, and have imported, tested, and backed them up, test going to the DoD Cyber Reporting site and logging in: https://dibnet.dod.mil/portal/intranet Click the Report button under Report a Cyber Incident. You will be taken away from this site to the https://dcise.cert.org/ site. At the prompt, choose the certificate you loaded into the browser, and type your Password/PIN.	
14.	Scroll to the bottom of the page and click **Mandatory Incident Report**.	

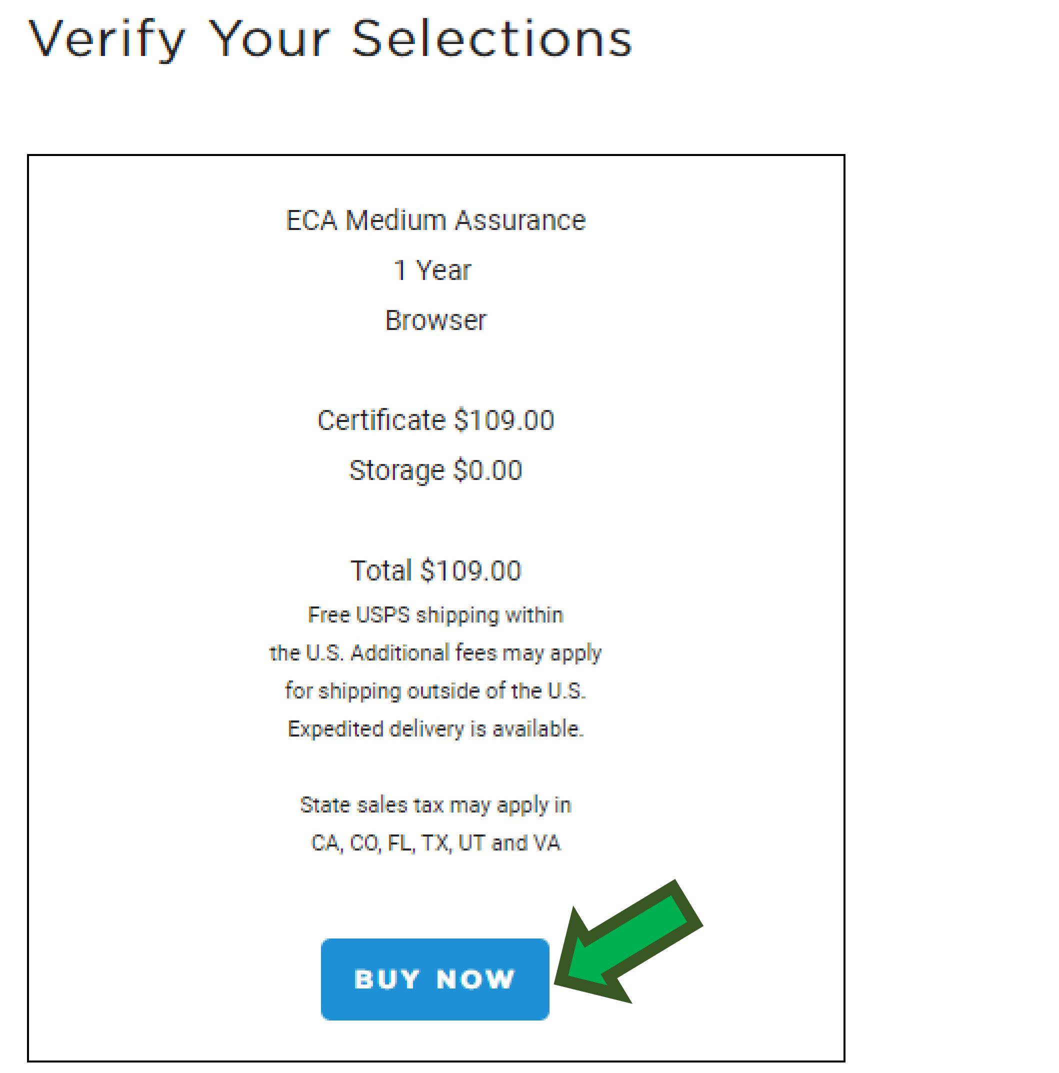
15.	If you can get to this page, you are set up to report cyber incidents. **DO NOT PROCEED FURTHER** unless you need to report an actual incident.	 Defense Industrial Base (DIB) Cyber Incident Reporting **Incident Collection Format** **Mandatory Incident Report** ***Questions marked with * are required.*** General Information · I. Company Identification · II. Company POC Information · III. Contract or Other Agreement · IV. Incident Information · V. Ancillary Information · Preview General Information Collection * Is this a follow-on report? [?] ○ Yes ○ No * Has this information been shared with any other Federal Government agency? ○ Yes ○ No Enter other tracking numbers (if applicable). * Does the network or information system affected contain or process information created by or for an element of the Intelligence Community? ○ Yes ○ No Cancel · Next
16.	**PROCEDURE FINISHED**	

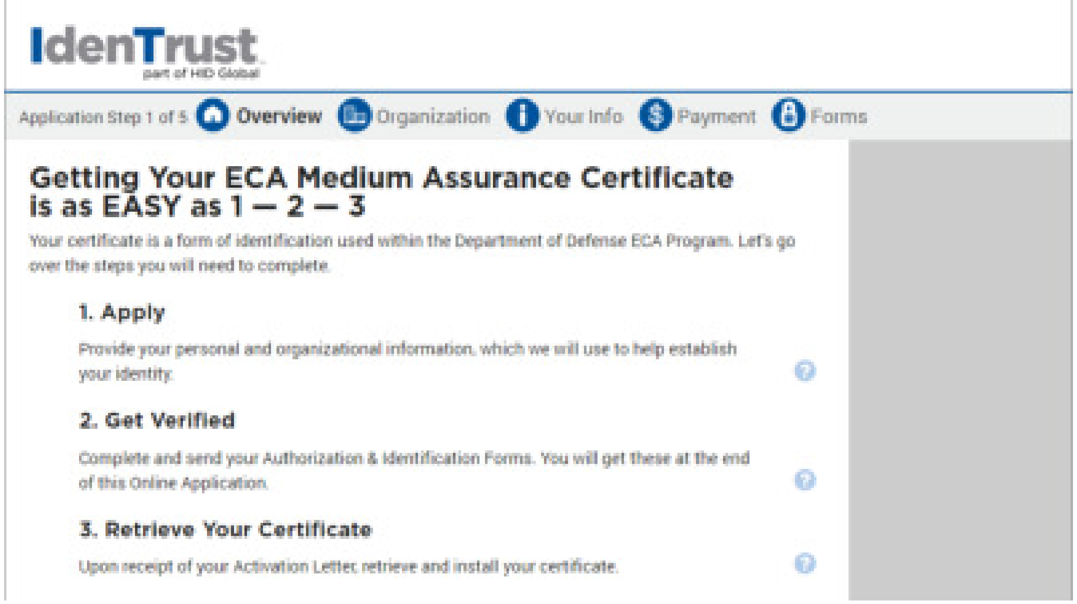
17.	If choosing the IdenTrust website, click the **IdenTrust** link.	 Approved ECA Vendors - Operational Research Consultants, Inc. (ORC) - IdenTrust, Inc.
18.	Click **OK** at the Exit Notice.	 Exit Notice: The appearance of hyperlinks does not constitute endorsement by the Defense Information Systems Agency of non-U.S. Government sites or the information, products, or services contained therein. Although the Defense Information Systems Agency may or may not use these sites as additional distribution channels for Department of Defense information, it does not exercise editorial control over all of the information that you may find at these locations. Such links are provided consistent with the stated purpose of this website.
19.	Toward the top of the page, click the **Buy Now** button.	 Comply with mandates for secure access to DoD information systems The DoD has established the External Certification Authority (ECA) program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The ECA program is designed to provide the mechanism for these entities to securely communicate with the DoD and authenticate to DoD information systems. A comprehensive portfolio of DoD ECA digital certificates

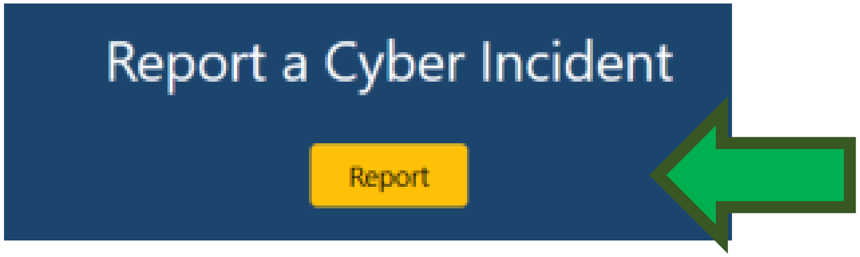
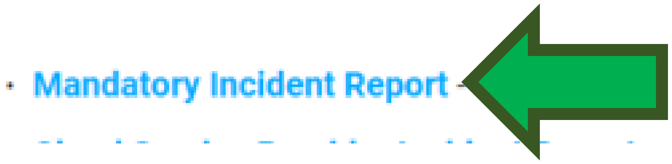
20.	Scroll down the list of DoD ECA Programs. Click the box for **DIB Cyber Incident Reporting.** Then click **Next.**	 Home · Help Me Choose If you will be using your DoD ECA certificate to access an agency application, you must specific the agency or agencies that you will use your certificate to interact with. We have worked with these agencies to determine the type of certificate(s) you can use with their application, which will be offered through the Certificate Selection Wizard. If you do not choose the appropriate agency you may not purchase the correct certificate type needed to access the agency application. If you do not see the agency on the list-don't worry, just select *My Federal Program is not Listed and you will be able to choose from a list of all DoD ECA certificates. **Please note that some agencies also accept IdenTrust Global Common (IGC) certificates. Based on your agency selection(s), options to purchase IGC certificates may also be offered to you.** If you would like to purchase a DoD ECA certificate and will not be interacting with a government agency, then select *No ECA Agency Affiliation is Required and you will be able to choose from a list of all DoD ECA certificates. DoD ECA Programs ☑ DIB Cyber Incident Reporting
21.	Click the box for **Yes.** Then click **Next.**	 I Live In The US ● Yes ○ No

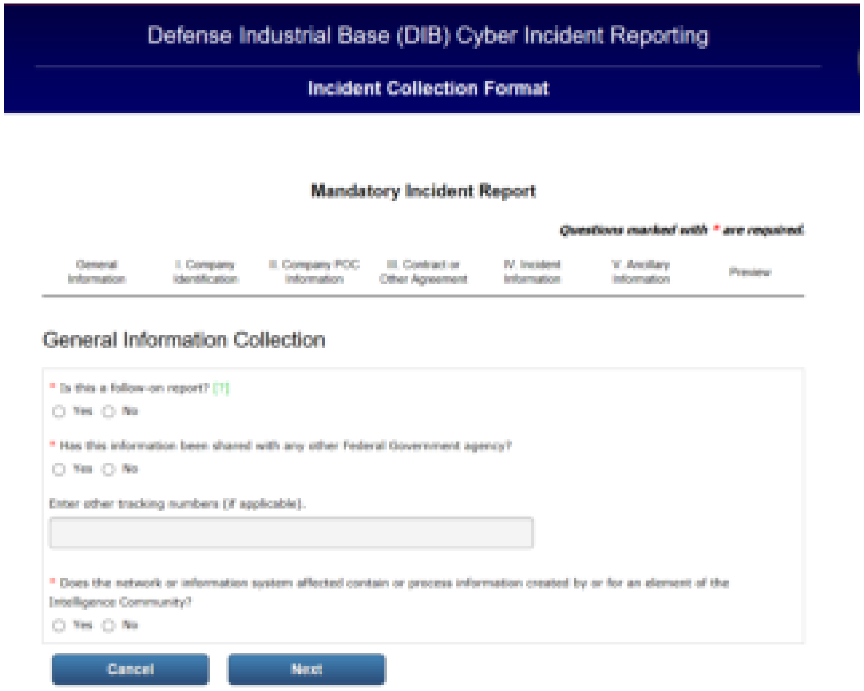
22.	Click the box for **ECA Medium Assurance.** Then click **Next.**	 Select A Certificate Please Select The Certificate Type You Would Like To Purchase ● ECA Medium Assurance $109.00 - $245.00 ○ ECA Medium Token Assurance $145.00 - $305.00 ○ ECA Medium Hardware Assurance $185.00 - $405.00

23.	Choose the length of certificate you wish to obtain. Leave the box for Browser checked. Then click **Next.**	 Please Select The Certificate Validity Period ● 1 Year - $109.00 ○ 2 Year - $195.00 ○ 3 Year - $245.00 Please Select The Storage Device For Your Certificate ● Browser -$0.00

24.	Verify your selection by clicking **Buy Now.**	 Verify Your Selections ECA Medium Assurance 1 Year Browser Certificate $109.00 Storage $0.00 Total $109.00 Free USPS shipping within the U.S. Additional fees may apply for shipping outside of the U.S. Expedited delivery is available. State sales tax may apply in CA, CO, FL, TX, UT and VA

25.	Continue through the application process. Here is a list of what you will need: • An official Photo ID: Driver's license or State ID Card • A Credit Card: In your name for address verification (not necessarily for payment) • Personal Information: Your FULL name (no nicknames or abbreviations), home address, and Social Security Number • Payment Information: Credit Card number or Payment Voucher number	 IdenTrust part of HID Global Application Step 1 of 5 Overview Organization Your Info Payment Forms Getting Your ECA Medium Assurance Certificate is as EASY as 1 — 2 — 3 Your certificate is a form of identification used within the Department of Defense ECA Program. Let's go over the steps you will need to complete. 1. Apply Provide your personal and organizational information, which we will use to help establish your identity. 2. Get Verified Complete and send your Authorization & Identification Forms. You will get these at the end of this Online Application. 3. Retrieve Your Certificate Upon receipt of your Activation Letter, retrieve and install your certificate.
26.	Useful tips and frequently asked questions are located here:	https://www.identrust.com/support/faq/24
27.	Turn-around time:	Per the website: Generally, certificate processing time takes 3-5 business days after your application is submitted and/or your required paperwork is received. If during the validation phase IdenTrust requires additional information, the process may take longer.

28.	Once you receive the certificates, and have imported, tested, and backed them up, test going to the DoD Cyber Reporting site and logging in: https://dibnet.dod.mil/portal/intranet Click the Report button under Report a Cyber Incident. You will be taken away from this site to the https://dcise.cert.org/ site. At the prompt, choose the certificate you loaded into the browser, and type your Password/PIN.	
29.	Scroll to the bottom of the page and click **Mandatory Incident Report**.	

30.	If you can get to this page, you are set up to report cyber incidents. **DO NOT PROCEED FURTHER** unless you need to report an actual incident.	 Defense Industrial Base (DIB) Cyber Incident Reporting **Incident Collection Format** **Mandatory Incident Report** ***Questions marked with * are required.*** General Information · I. Company Identification · II. Company POC Information · III. Contract or Other Agreement · IV. Incident Information · V. Ancillary Information · Preview General Information Collection * Is this a follow-on report? [?] ○ Yes ○ No * Has this information been shared with any other Federal Government agency? ○ Yes ○ No Enter other tracking numbers (if applicable). * Does the network or information system affected contain or process information created by or for an element of the Intelligence Community? ○ Yes ○ No Cancel · Next
31.	**PROCEDURE FINISHED**	