# CYBERSECURITY REGULATIONS OVERVIEW

NORTH CAROLINA MILITARY BUSINESS CENTER

10 JANUARY 2022

# WHAT IS CYBERSECURITY?

**Computer security, cybersecurity, or information technology security is the *protection* of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. - Wikipedia**

# WHY IS CYBERSECURITY SO IMPORTANT?

Our adversaries want our data and/or to disrupt our supply chains**. *Data is the new currency and loss of function is the new weapon.***

- For decades China's strategy has been to rely on intellectual property theft to develop their weapons. China's J-31 Stealth Fighter is a replica of our F-35 Joint Strike Fighter – including the design flaw.

- Russia steals our IP, but they also want to disrupt our supply chains, our economy and our political system to make us look like the Keystone Kops.

***Our adversaries also want our 'dirt'. If we don't keep our data out of their hands, we are at risk of being forced to speak a foreign language and embrace a foreign culture.***

# CYBERSECURITY STATISTICS

- Cybercrime will cost the world economy $10.5 trillion by 2025.

- Cybercrime is more profitable than the global drug trade.

- A business becomes a victim of ransomware every 11 seconds.

- By 2023 there will be 3 times more networked devices than humans.

- 43% of cyber attacks target small businesses and 60% of them will go out of business within 6 months.

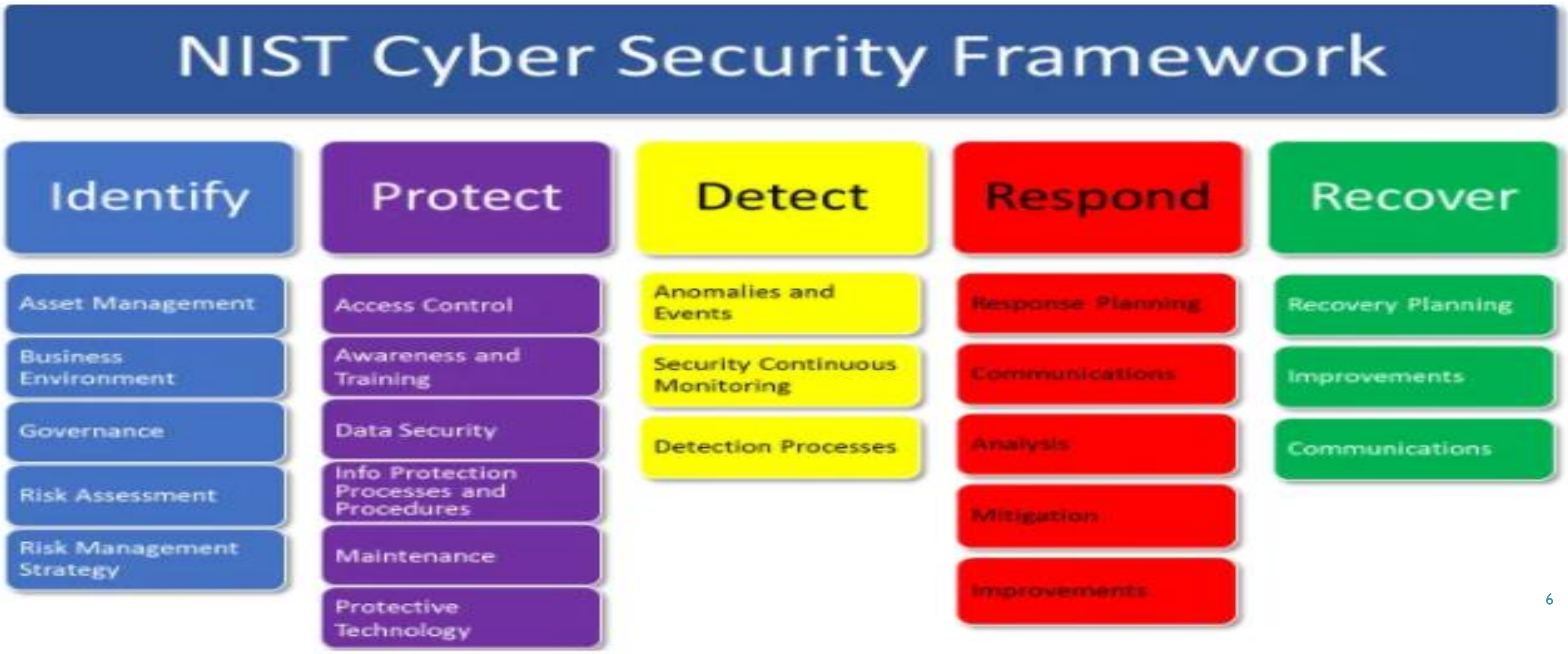
# REGULATION VS CLAUSE VS FRAMEWORK

Is it a regulation, a clause, or a framework?

A clause is a section of a regulation, and they are not the same thing as a framework. It can be confusing becomes the terms are often used interchangeably.

**Example:** NIST SP 800-171 is a cybersecurity **framework** that was developed by the National Institute of Standards and Technology (NIST). The 'SP' is an acronym for Special Publication. NIST SP 800-171 is referenced in DFARS – Defense Federal Acquisition **Regulation** Supplement – **clause** 252.204-7012. The DoD requires that defense contractors protect sensitive data by implementing the 110 cybersecurity controls and the Non-Federal Organization (NFO) controls in the NIST SP 800-171 **framework**.

# NIST SP 800-171 CYBERSECURITY FRAMEWORK



## NIST Cyber Security Framework

| Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|
| Asset Management | Access Control | Anomalies and Events | Response Planning | Recovery Planning |
| Business Environment | Awareness and Training | Security Continuous Monitoring | Communications | Improvements |
| Governance | Data Security | Detection Processes | Analysis | Communications |
| Risk Assessment | Info Protection Processes and Procedures | | Mitigation | |
| Risk Management Strategy | Maintenance | | Improvements | |
| | Protective Technology | | | |

# CYBERSECURITY REGULATIONS

Over the past decade, the Federal Government has released multiple regulations aimed at protecting our nation's sensitive data. The FAR/DFARS clauses discussed in this section are the ones most often seen in solicitations and contracts. Be sure to check your contracts for other cybersecurity regulations.

**FAR 52.204-21** – Basic Safeguarding of Covered Contractor Information Systems.

- List of 15 basic cybersecurity controls that apply to all federal contractors with Federal Contract Information (FCI) residing in or transiting through their information systems. Is not applicable for COTS items or items purchased under the micro-threshold limit.
- Requires contractors to include the clause in subcontracts if subcontractor 'touches' FCI.
- No provision for audits/assessments. Contractors self-attest to compliance.
- Does not reference a framework to use for compliance.

# CYBERSECURITY REGULATIONS

**FAR 52.204-23** -Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by **Kaspersky Lab** and Other Covered Entities.

- If a contractor identifies a covered article provided to the Government during contract performance, the contractor shall report, in writing, to the Contracting Officer. *Note: DoD contractors must also report using the website: https://dibnet.dod.mil.*
- Within 1 business day from the date of the identification, the contractor must report the contract number, the order number(s), supplier name, brand, model number manufacturer part number, item description and any information about mitigation actions undertaken or recommended.
- Within 10 business days of submitting the report, the contractor shall report any further information about mitigations actions undertaken or recommended and describe the efforts it undertook to prevent use or submission of a covered articles and how it intends to prevent use or submission in the future.
- This clause must be inserted in all subcontracts – **including for the acquisition of COTS.**

# CYBERSECURITY REGULATIONS

**FAR 52.204-25** - Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Huawei Technologies, ZTE Corp., Hytera Communications, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company)

- If a contractor identifies a covered article provided to the Government during contract performance, the contractor shall report, in writing, to the Contracting Officer. *Note: DoD contractors must also report using the website: https://dibnet.dod.mil.*
- Within 1 business day from the date of the identification, the contractor must report the contract number, the order number(s), supplier name, brand, model number manufacturer part number, item description and any information about mitigation actions undertaken or recommended.
- Within 10 business days of submitting the report, the contractor shall report any further information about mitigations actions undertaken or recommended and describe the efforts it undertook to prevent use or submission of a covered articles and how it intends to prevent use or submission in the future.
- This clause must be inserted in all subcontracts – **including for the acquisition of COTS.**

# CYBERSECURITY REGULATIONS

**DFARS 252.204-7008** – Compliance with Safeguarding Covered Defense Information Controls Act.

- If the offeror proposes to vary from any of the requirements specified in the NIST SP 800-171 framework, the offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO) a written explanation of why a particular security requirement is not applicable or how an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.
- Offeror requests will be adjudicated **prior** to contract award.
- Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.
- No flow-down to subs – variances apply only to the contractor named in the contract.

NOTE: This clause is only applicable to contractors that process, transmit, store, and/or create controlled unclassified information (CUI) in the performance of the contract. By accepting the contract, the contractor is self-attesting to compliance with the cybersecurity controls in NIST SP 800-171.

# CYBERSECURITY REGULATIONS

**DFARS 252.204-7012** – Safeguarding Covered Defense Information and Cyber Incident Reporting.

- Contractors' information systems must comply with the 110 cybersecurity controls, AND the Non-Federal Organization (NFO) controls in NIST SP 800-17.
- External cloud service providers that store, process or transmit controlled unclassified information (CUI) on behalf of a contractor must meet security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.
- In the event of a cyber incident, the contractor shall identify compromised computers, servers, and user accounts and report the incident within 72 hours to the DoD at https://dibnet.dod.mil.
- A Medium Assurance Certificate is required to report cyber incidents. (instructions begin on slide 20)
- Malicious software must be submitted to the DoD Cyber Crime Center (DC#) in accordance with instructions. **Do not send malicious software to the Contracting Officer.**

# CYBERSECURITY REGULATIONS

DFARS 252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting

- Contractor shall preserve and protect images of all known affected information systems and all monitoring/packet capture data for at least 90 days from the submission of the cyber incident.
- Upon request by the DoD, the contractor shall provide access to additional information or equipment that is necessary to conduct a forensic analysis – which could include proprietary information which the DoD is required to protect.
- This clause must be flowed down to subcontractors that will 'touch' CUI.

NOTE: This clause is only applicable to contractors that process, transmit, store, and/or create controlled unclassified information (CUI) in the performance of the contract – even if the clause is referenced in your contract. By accepting the contract, the contractor is **self-attesting** to compliance with the cybersecurity controls in the NIST SP 800-171 framework.

# CYBERSECURITY REGULATIONS

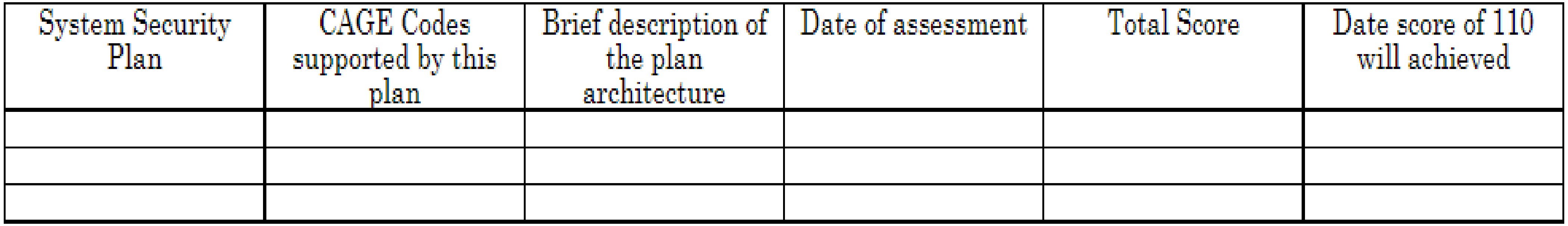
In November of 2020, the DoD released the DFARS Interim Rule which added 3 additional cybersecurity clauses.

1. DFARS 252.204-7019 – Notice of NIST SP 800-171 DoD Assessment Requirements

   - ✓ Added additional requirements to DFARS 252.204-7012
   - ✓ Defense contractors must perform a self-assessment (Basic Assessment) of their information system to determine compliance to the NIST SP 800-171 framework. Contractors must use the DoD Assessment Methodology to determine the score.
   - ✓ Contractors should use NIST SP 800-171A – Assessing Security Requirements for CUI – to perform their self-assessment against the assessment objectives for each control.
   - ✓ Self-assessment scores must be reported using the Supplier Performance Risk System (SPRS).
   - ✓ Flow-down requirements are not explicit but are implied in DFARS 252.204-7020.

# CYBERSECURITY REGULATIONS

- DFARS 252.204-7019 – Notice of NIST SP 800-171 DoD Assessment Requirements (cont’d)
  - ✓ Self-Assessments must be performed every 3 years
  - ✓ A score may not be posted in SPRS unless a System Security Plan has been completed.
  - ✓ Plans of Action and Milestones (POAMs) are allowed for controls that have not yet been implemented.
  - ✓ Applies to contractors that ‘touch’ CUI



| System Security Plan | CAGE Codes supported by this plan | Brief description of the plan architecture | Date of assessment | Total Score | Date score of 110 will achieved |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

# CYBERSECURITY REGULATIONS

2. DFARS 252.204-7020 – NIST SP 800-171 DoD Assessment Requirements
   - ✓ Added additional requirements to DFARS 252.204-7012
   - ✓ The contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment.
   - ✓ The DoD will provide Medium and High Assessment summary level scores to the contractor and offer opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the scores in SPRS.
   - ✓ Applies to contractors that 'touch' CUI
   - ✓ Clause must be flowed down to subcontractors that 'touch' CUI

***Go to the DFARS tab on the cyberNC.us website for additional information about the DFARS Interim Rule.***

# CYBERSECURITY REGULATIONS

3. DFARS 252.204-7021 – Cybersecurity Maturity Model Certification Requirements

   ✓ Implemented the CMMC *framework*

   ✓ No longer applicable since CMMC 2.0 was released in November of 2021 and must go through the rule-making process.

***For more information about CMMC 2.0 go to the CMMC tab on the cyberNC.us website.***

# AVOID CUI!

Implementing a cybersecurity program that is compliant with NIST 800-171 is expensive, time-consuming, and complex – particularly for small contractors.

Every piece of sensitive data that is on or transmitted by a contractor's network puts national security at risk. We need to do a better job of keeping sensitive data out of cyberspace.

*How do we do that?*

- *Only flow down the data that is essential to perform the work. An entire technical data package does not need to be sent to a machine shop that is fabricating nuts and bolts.*
- *Work with your contracting officers/primes/subs to find ways to keep sensitive data out of cyberspace.*
  - ✓ *If only one document that contains sensitive data is needed, consider using USPS, FedEx or UPS.*
  - ✓ *Redact sensitive data prior to sending.*

# NATIONAL SECURITY

We all need to do our part to protect national security; it is our patriotic duty as citizens of this country.

# CYBERSECURITY REGULATIONS OVERVIEW

NORTH CAROLINA MILITARY BUSINESS CENTER

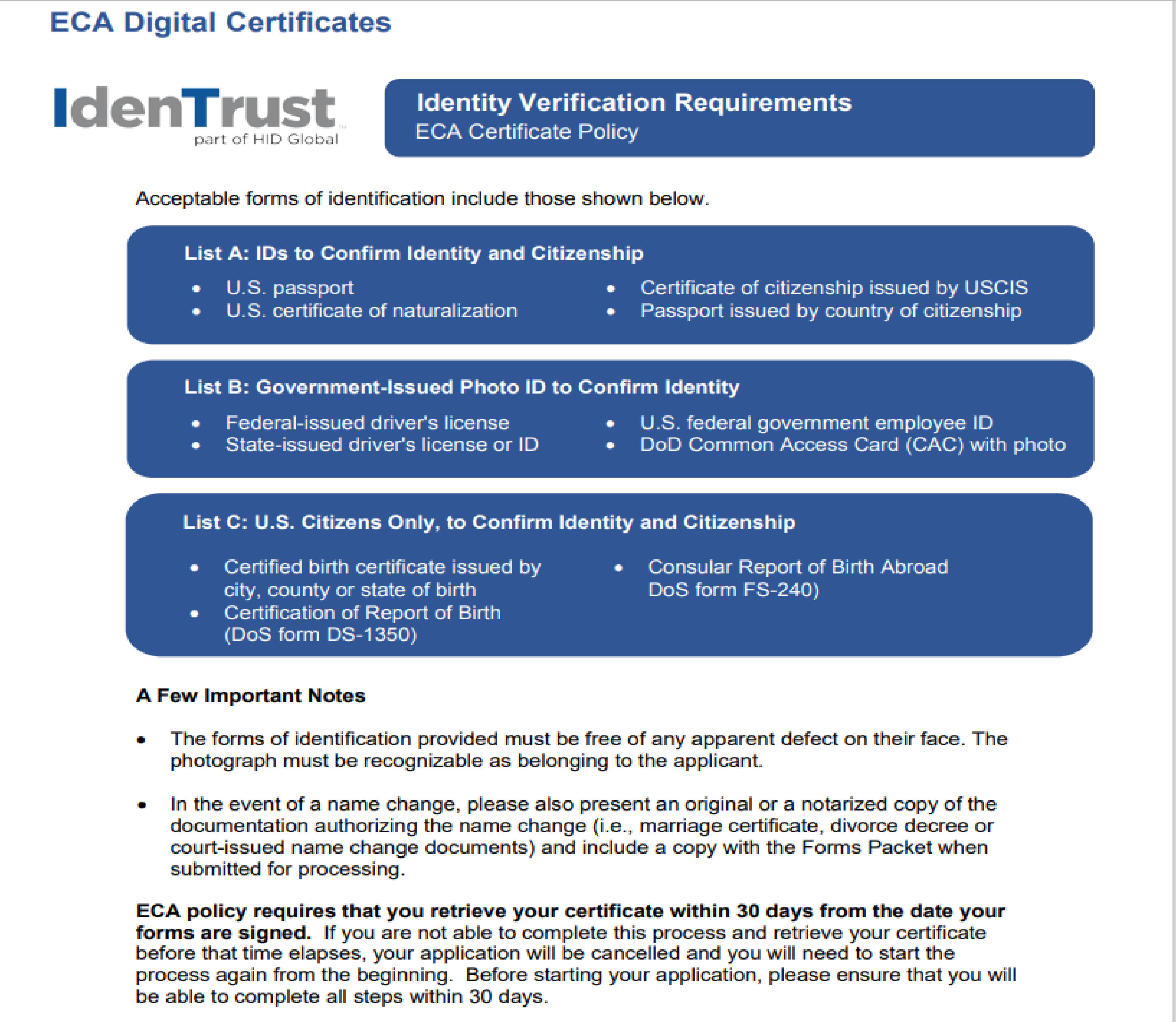
10 JANUARY 2022

# MEDIUM ASSURANCE CERTIFICATE

DFARS 252.204-7012 requires that contractors have a Medium Assurance Certificate to report cyber incidents via https://dibnet.dod.mil.

- It takes at least 3 to 5 days to process the information needed to get a certificate, so you can't wait until you experience a cyber incident to apply for a Medium Assurance Certificate. You need to apply now.
- If you have a CAC card you do not need a certificate.
- Certificates are not free, and you may need to consider purchasing more than one. Latest price: $114

*Detailed instructions begin on the next slide.*



ECA Digital Certificates

IdenTrust part of HID Global

## Identity Verification Requirements

ECA Certificate Policy

Acceptable forms of identification include those shown below.

**List A: IDs to Confirm Identity and Citizenship**

- U.S. passport
- U.S. certificate of naturalization
- Certificate of citizenship issued by USCIS
- Passport issued by country of citizenship

**List B: Government-Issued Photo ID to Confirm Identity**

- Federal-issued driver's license
- State-issued driver's license or ID
- U.S. federal government employee ID
- DoD Common Access Card (CAC) with photo

**List C: U.S. Citizens Only, to Confirm Identity and Citizenship**

- Certified birth certificate issued by city, county or state of birth
- Certification of Report of Birth (DoS form DS-1350)
- Consular Report of Birth Abroad DoS form FS-240)

**A Few Important Notes**

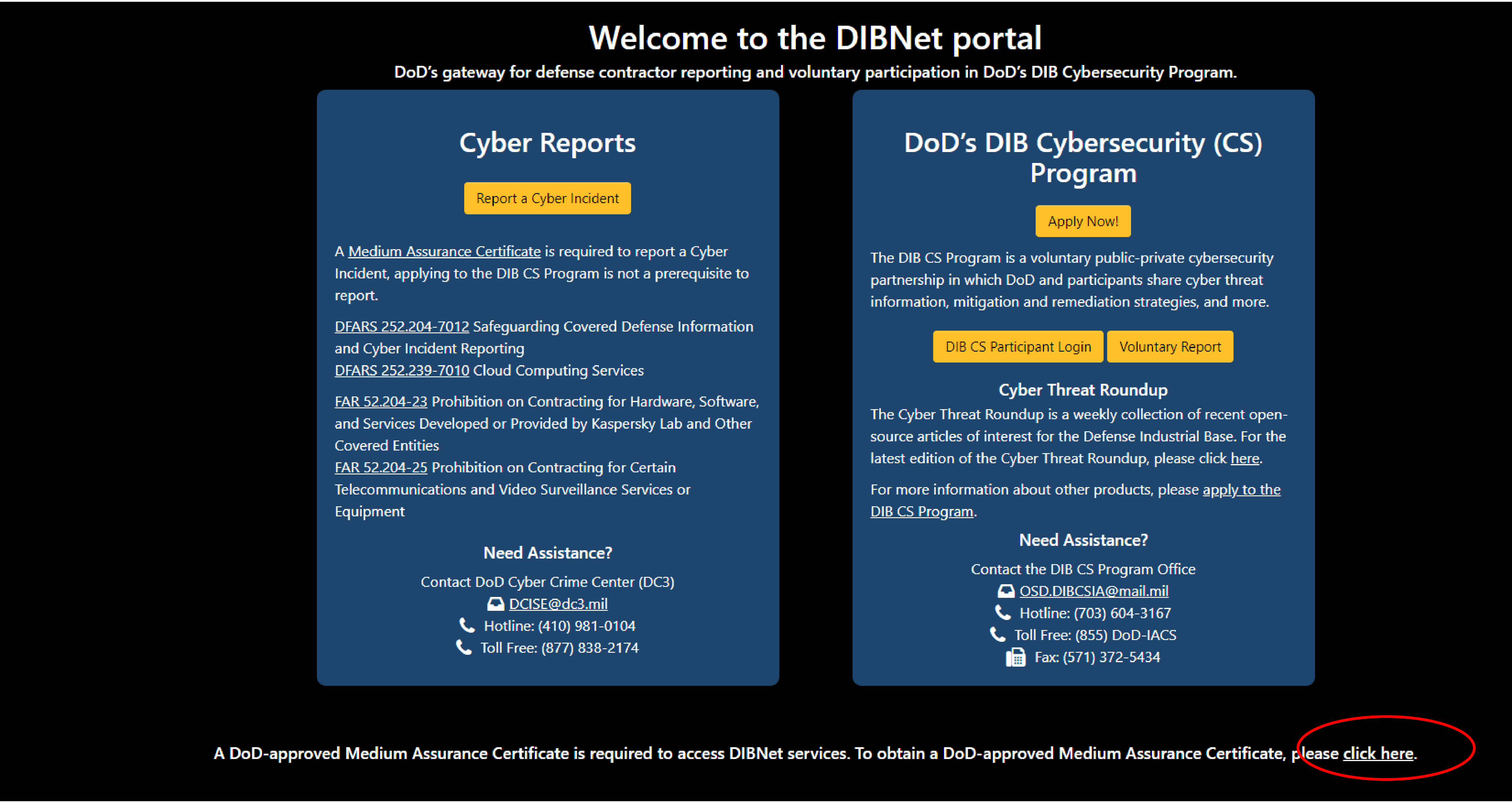
- The forms of identification provided must be free of any apparent defect on their face. The photograph must be recognizable as belonging to the applicant.
- In the event of a name change, please also present an original or a notarized copy of the documentation authorizing the name change (i.e., marriage certificate, divorce decree or court-issued name change documents) and include a copy with the Forms Packet when submitted for processing.

**ECA policy requires that you retrieve your certificate within 30 days from the date your forms are signed.** If you are not able to complete this process and retrieve your certificate before that time elapses, your application will be cancelled and you will need to start the process again from the beginning. Before starting your application, please ensure that you will be able to complete all steps within 30 days.

What you need:

- Two forms of ID – one must be a picture ID
- HQ address for your organization
- Name of agency - Dept. of Defense
- Credit card to pay for the certificate

At the end of the application process, you will be provided with Authentication & Identification forms – they must be notarized.



# Welcome to the DIBNet portal

DoD's gateway for defense contractor reporting and voluntary participation in DoD's DIB Cybersecurity Program.

## Cyber Reports

A Medium Assurance Certificate is required to report a Cyber Incident, applying to the DIB CS Program is not a prerequisite to report.

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
DFARS 252.239-7010 Cloud Computing Services

FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities
FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

### Need Assistance?

Contact DoD Cyber Crime Center (DC3)
✉ DCISE@dc3.mil
☎ Hotline: (410) 981-0104
☎ Toll Free: (877) 838-2174

## DoD's DIB Cybersecurity (CS) Program

The DIB CS Program is a voluntary public-private cybersecurity partnership in which DoD and participants share cyber threat information, mitigation and remediation strategies, and more.

### Cyber Threat Roundup

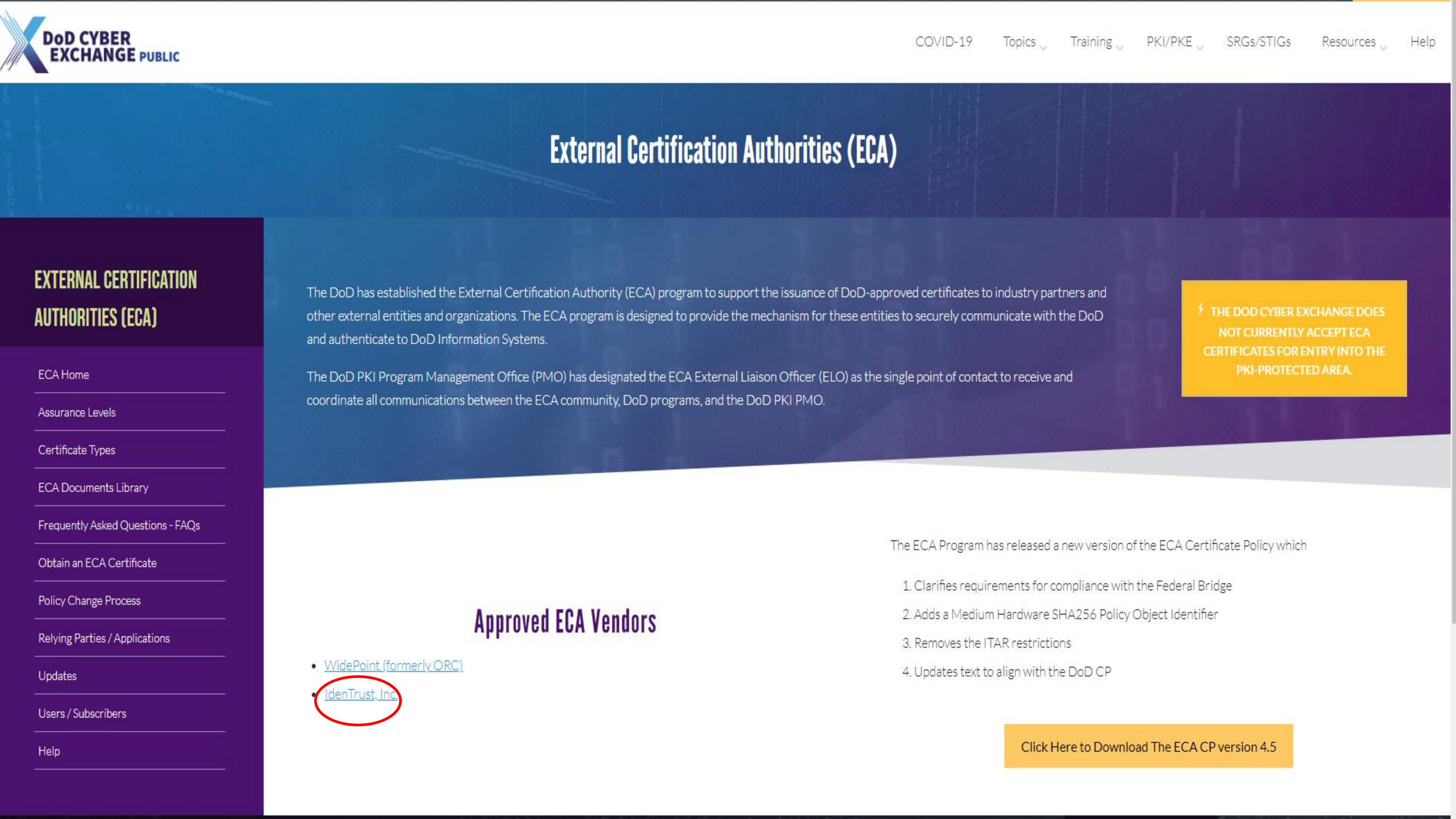
The Cyber Threat Roundup is a weekly collection of recent open-source articles of interest for the Defense Industrial Base. For the latest edition of the Cyber Threat Roundup, please click here.

For more information about other products, please apply to the DIB CS Program.

### Need Assistance?

Contact the DIB CS Program Office
✉ OSD.DIBCSIA@mail.mil
☎ Hotline: (703) 604-3167
☎ Toll Free: (855) DoD-IACS
📠 Fax: (571) 372-5434

A DoD-approved Medium Assurance Certificate is required to access DIBNet services. To obtain a DoD-approved Medium Assurance Certificate, please click here.



# External Certification Authorities (ECA)

## EXTERNAL CERTIFICATION AUTHORITIES (ECA)

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.

The DoD PKI Program Management Office (PMO) has designated the ECA External Liaison Officer (ELO) as the single point of contact to receive and coordinate all communications between the ECA community, DoD programs, and the DoD PKI PMO.

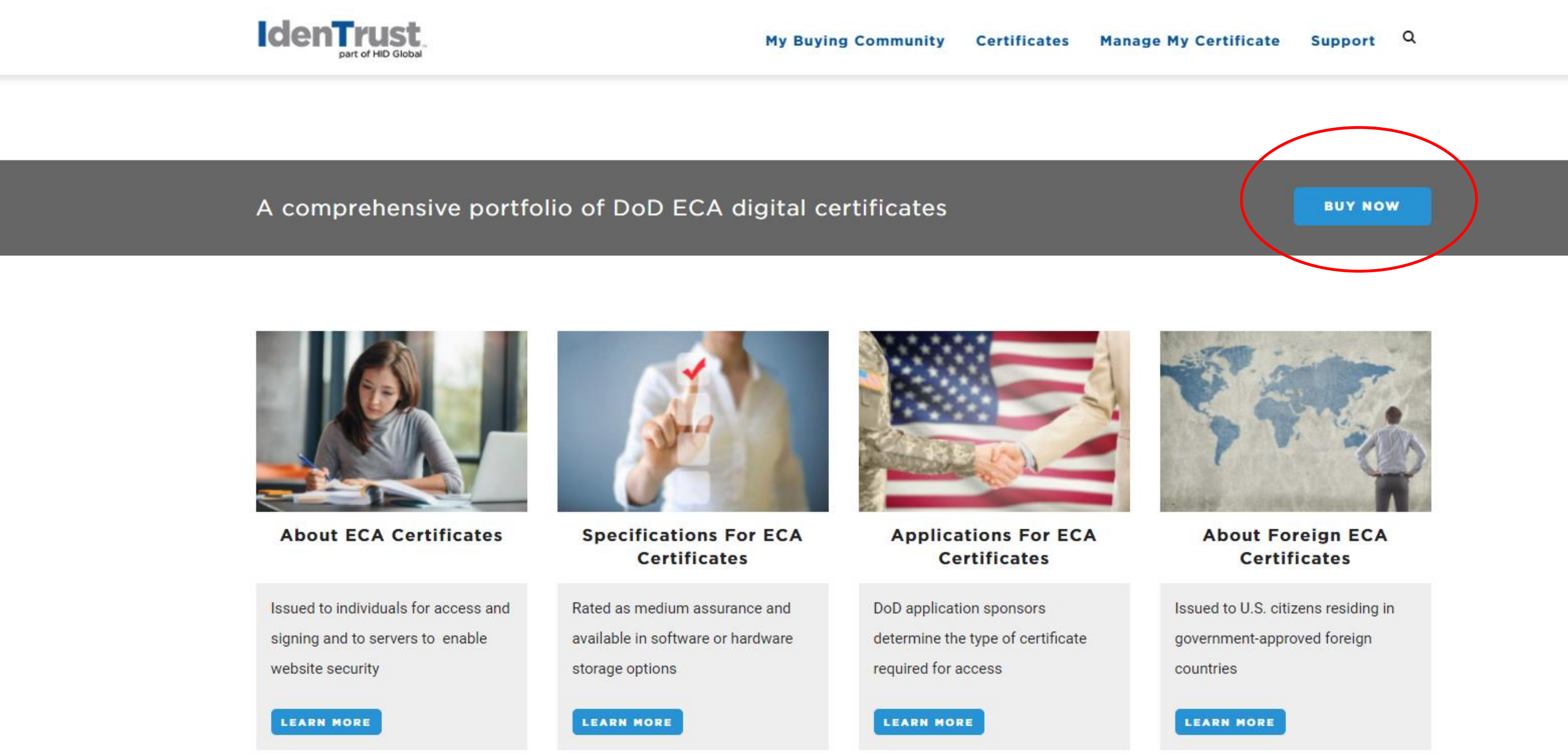
THE DOD CYBER EXCHANGE DOES NOT CURRENTLY ACCEPT ECA CERTIFICATES FOR ENTRY INTO THE PKI-PROTECTED AREA.

## Approved ECA Vendors

- WidePoint (formerly ORC)
- IdenTrust, Inc.

The ECA Program has released a new version of the ECA Certificate Policy which

1. Clarifies requirements for compliance with the Federal Bridge
2. Adds a Medium Hardware SHA256 Policy Object Identifier
3. Removes the ITAR restrictions
4. Updates text to align with the DoD CP



A comprehensive portfolio of DoD ECA digital certificates

### About ECA Certificates

Issued to individuals for access and signing and to servers to enable website security

### Specifications For ECA Certificates

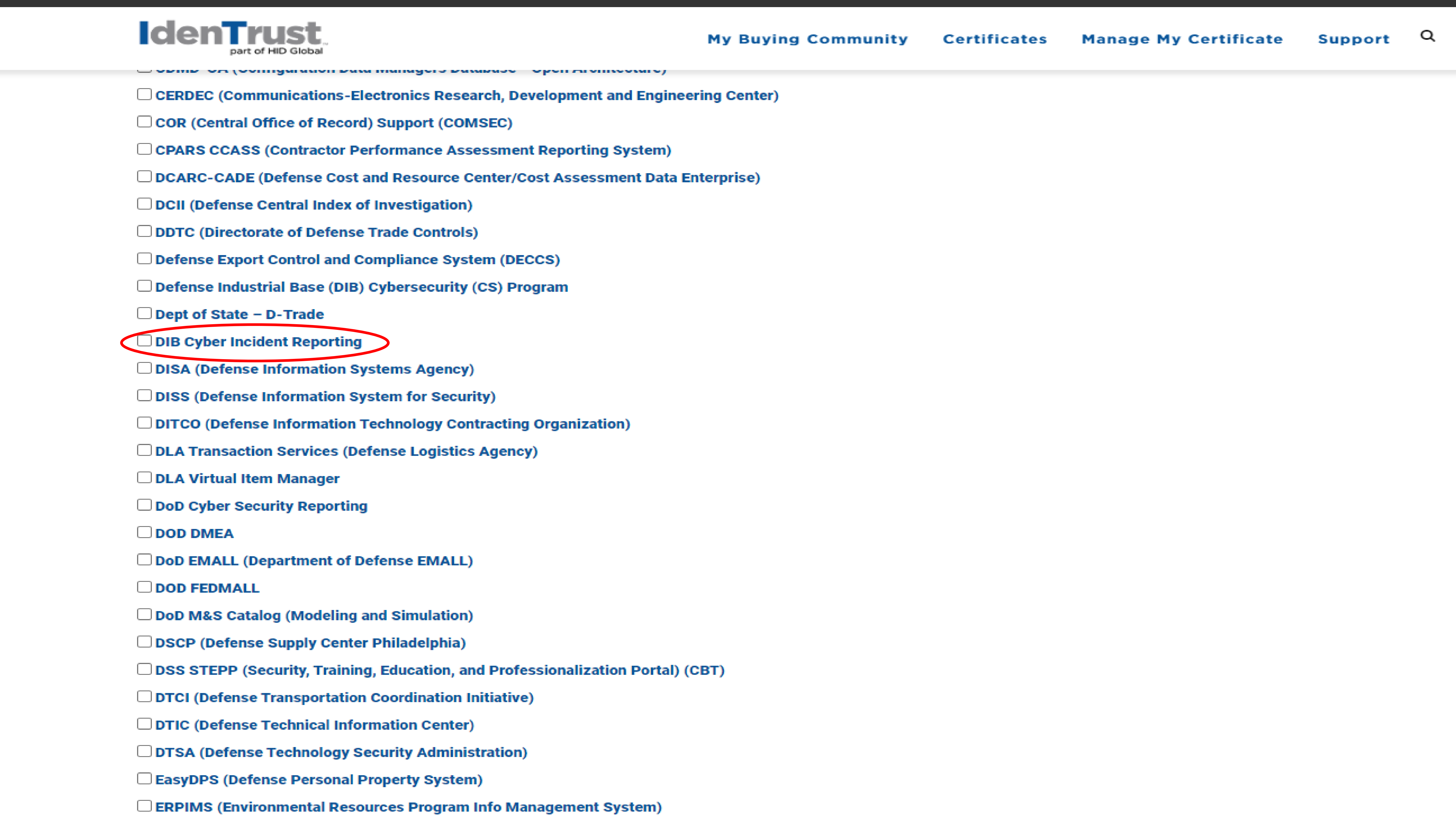
Rated as medium assurance and available in software or hardware storage options

### Applications For ECA Certificates

DoD application sponsors determine the type of certificate required for access

### About Foreign ECA Certificates

Issued to U.S. citizens residing in government-approved foreign countries



IdenTrust
part of HID Global

My Buying Community    Certificates    Manage My Certificate    Support

□ CDMD-OA (Configuration Data Managers Database – Open Architecture)

□ CERDEC (Communications-Electronics Research, Development and Engineering Center)

□ COR (Central Office of Record) Support (COMSEC)

□ CPARS CCASS (Contractor Performance Assessment Reporting System)

□ DCARC-CADE (Defense Cost and Resource Center/Cost Assessment Data Enterprise)

□ DCII (Defense Central Index of Investigation)

□ DDTC (Directorate of Defense Trade Controls)

□ Defense Export Control and Compliance System (DECCS)

□ Defense Industrial Base (DIB) Cybersecurity (CS) Program

□ Dept of State – D-Trade

□ DIB Cyber Incident Reporting

□ DISA (Defense Information Systems Agency)

□ DISS (Defense Information System for Security)

□ DITCO (Defense Information Technology Contracting Organization)

□ DLA Transaction Services (Defense Logistics Agency)

□ DLA Virtual Item Manager

□ DoD Cyber Security Reporting

□ DOD DMEA

□ DoD EMALL (Department of Defense EMALL)

□ DOD FEDMALL

□ DoD M&S Catalog (Modeling and Simulation)

□ DSCP (Defense Supply Center Philadelphia)

□ DSS STEPP (Security, Training, Education, and Professionalization Portal) (CBT)

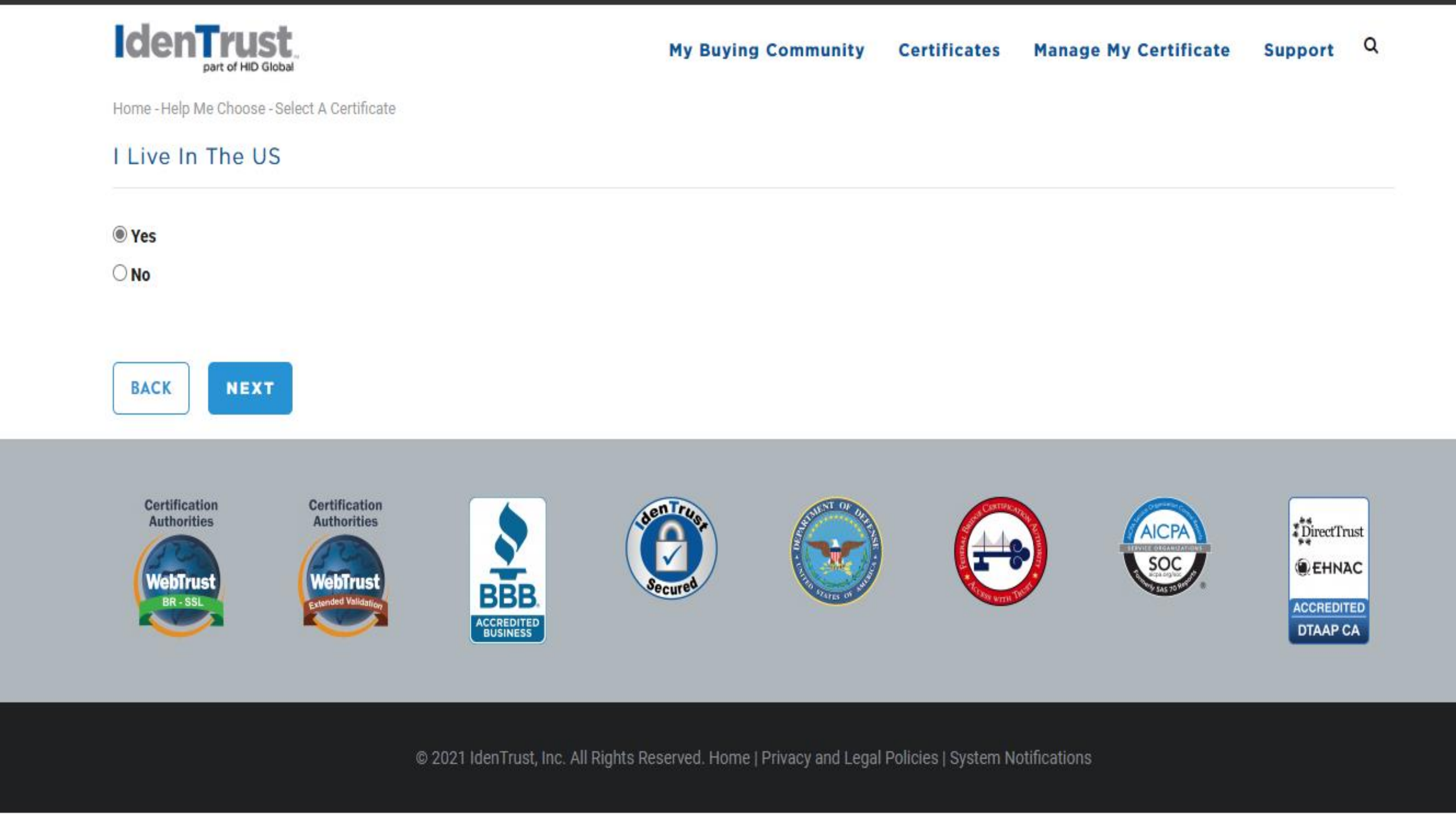
□ DTCI (Defense Transportation Coordination Initiative)

□ DTIC (Defense Technical Information Center)

□ DTSA (Defense Technology Security Administration)

□ EasyDPS (Defense Personal Property System)

□ ERPIMS (Environmental Resources Program Info Management System)



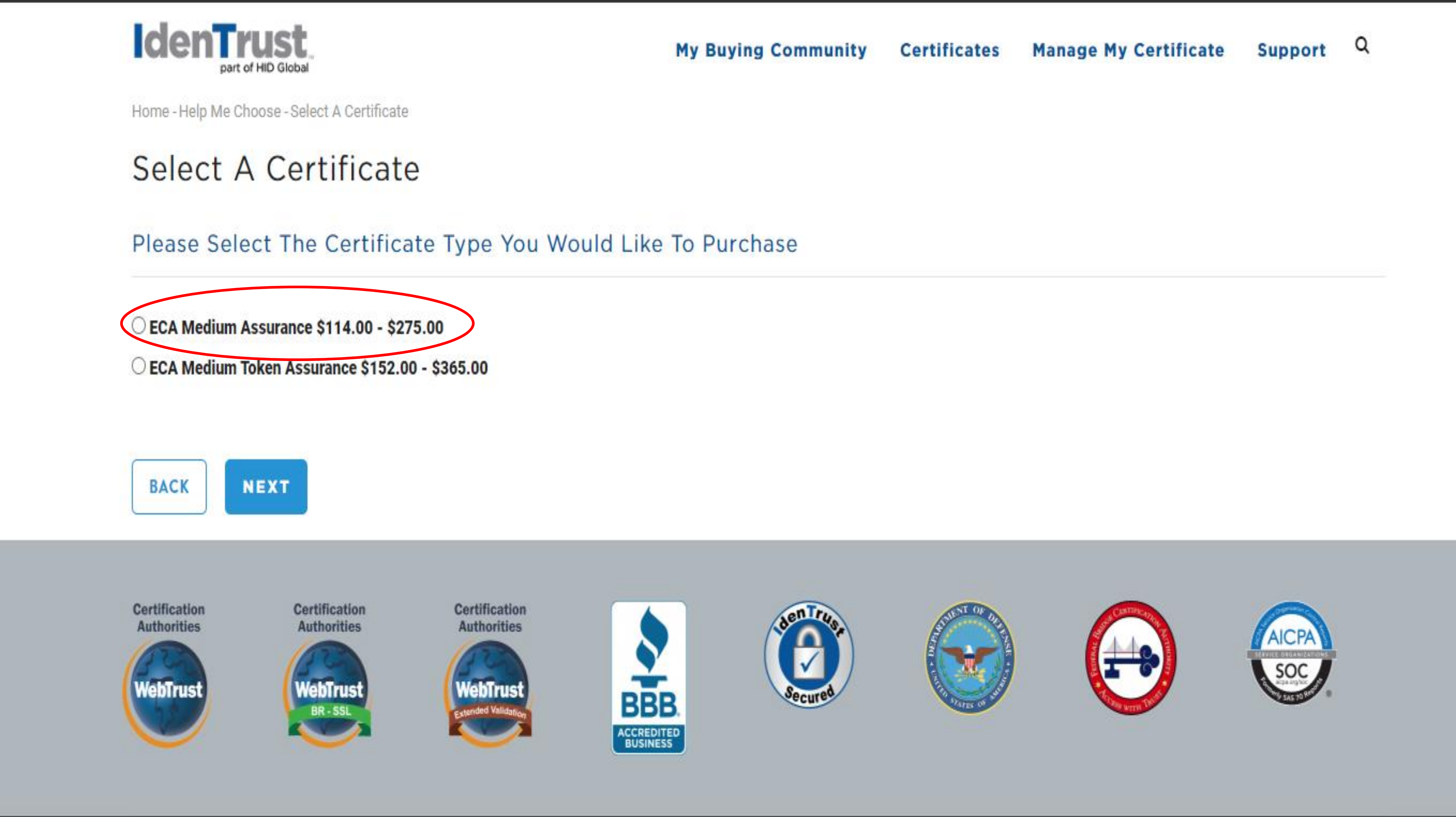
Home - Help Me Choose - Select A Certificate

## I Live In The US

● Yes

○ No

© 2021 IdenTrust, Inc. All Rights Reserved. Home | Privacy and Legal Policies | System Notifications

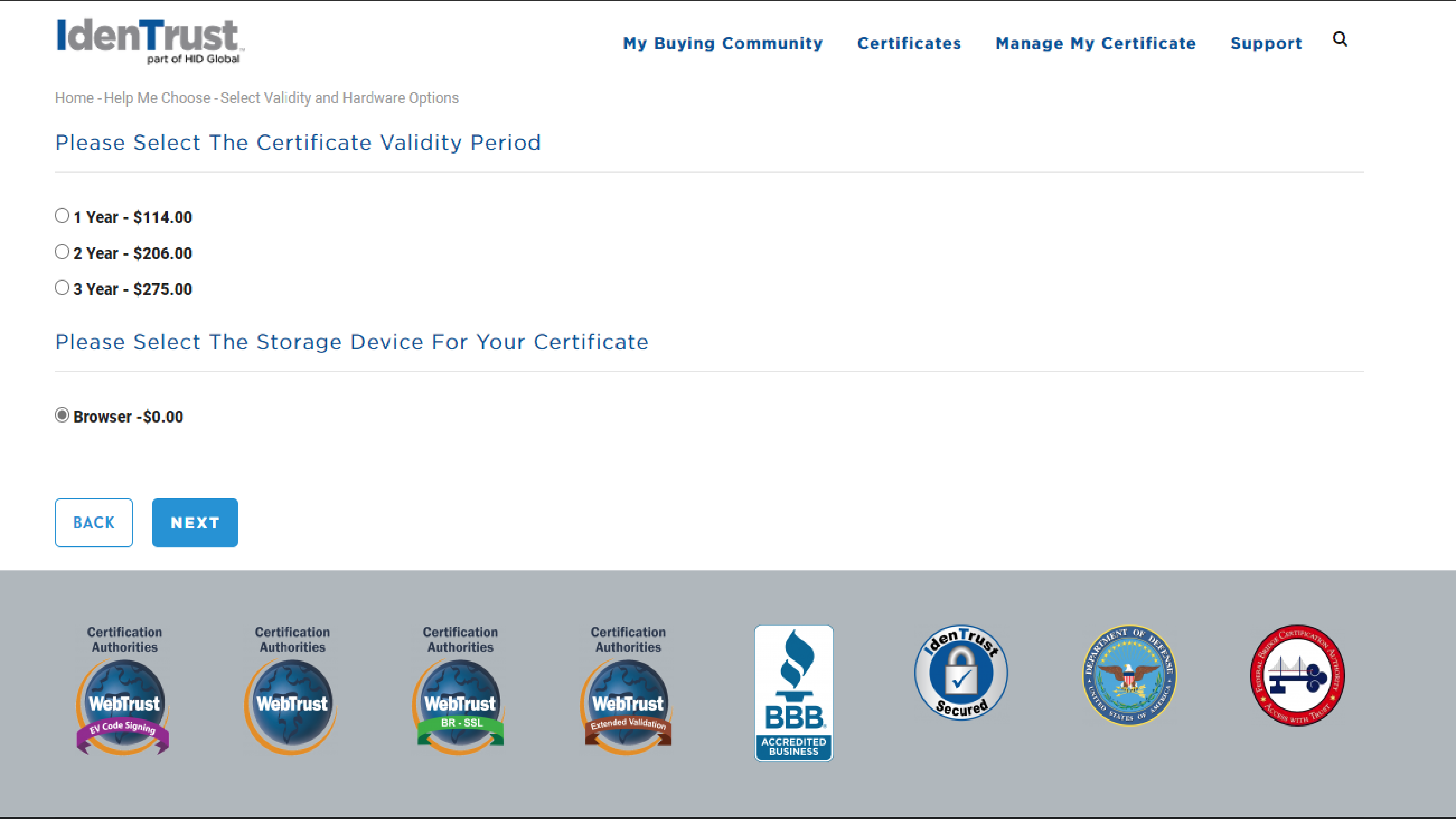


# Select A Certificate

## Please Select The Certificate Type You Would Like To Purchase

[✓ ○ ECA Medium Assurance $114.00 - $275.00]

○ ECA Medium Token Assurance $152.00 - $365.00



IdenTrust
part of HID Global
My Buying Community
Certificates
Manage My Certificate
Support
Home - Help Me Choose - Select Validity and Hardware Options

## Please Select The Certificate Validity Period

○ 1 Year - $114.00

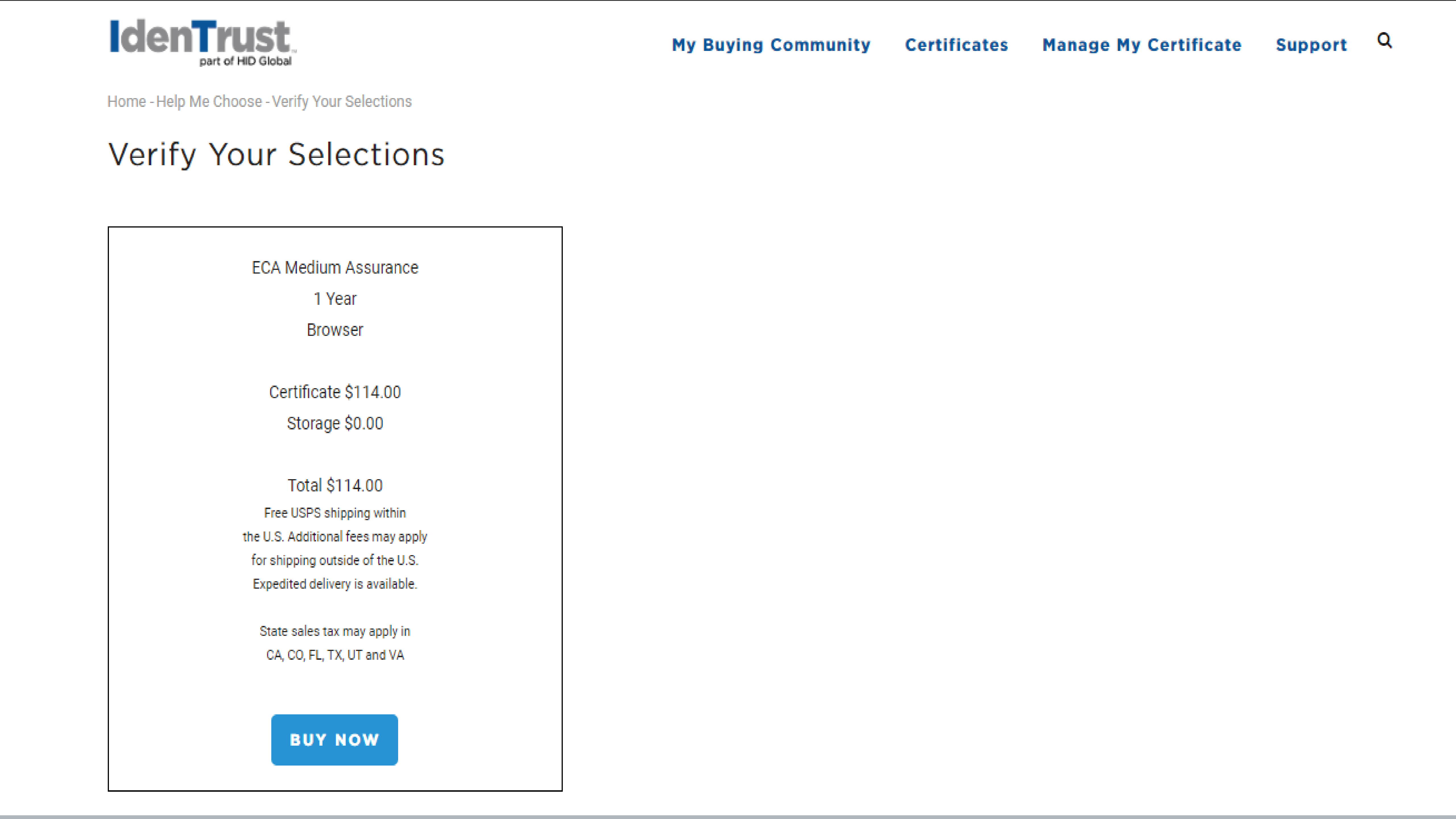
○ 2 Year - $206.00

○ 3 Year - $275.00

## Please Select The Storage Device For Your Certificate

● Browser -$0.00

BACK
NEXT
Certification Authorities WebTrust EV Code Signing
Certification Authorities WebTrust
Certification Authorities WebTrust BR - SSL
Certification Authorities WebTrust Extended Validation
BBB ACCREDITED BUSINESS
IdenTrust Secured



Home - Help Me Choose - Verify Your Selections

# Verify Your Selections

ECA Medium Assurance

1 Year

Browser

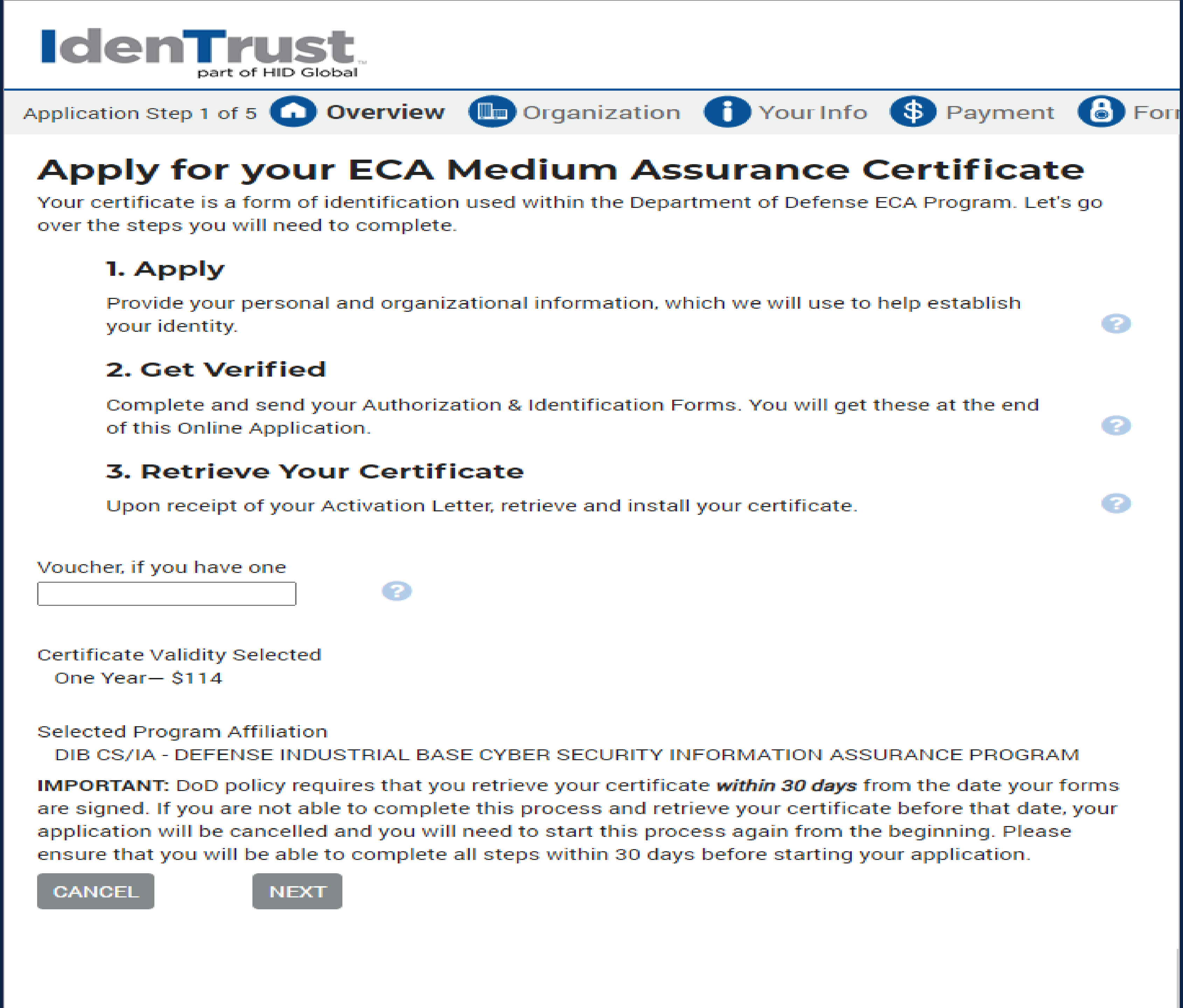
Certificate $114.00

Storage $0.00

Total $114.00

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



# Apply for your ECA Medium Assurance Certificate

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.

Voucher, if you have one

Certificate Validity Selected
One Year— $114

Selected Program Affiliation
DIB CS/IA - DEFENSE INDUSTRIAL BASE CYBER SECURITY INFORMATION ASSURANCE PROGRAM

**IMPORTANT:** DoD policy requires that you retrieve your certificate ***within 30 days*** from the date your forms are signed. If you are not able to complete this process and retrieve your certificate before that date, your application will be cancelled and you will need to start this process again from the beginning. Please ensure that you will be able to complete all steps within 30 days before starting your application.

# MEDIUM ASSURANCE CERTIFICATE

- Once the certificates have been imported, tested and back up, perform a test by going to the DoD Cyber Reporting site and clicking on the Report a Cyber Incident button.
  - ✓ You will be taken to the https://dcise.cert.org/ site. At the prompt, choose the certificate you loaded into the browser, and type your Password/PIN
  - ✓ Scroll to the bottom of the page and click Mandatory Incident Report
  - ✓ If you get to the Incident Collection Format page, you are set up to report cyber incidents.
  - ✓ ***Do not proceed further unless you're reporting an actual incident.***