DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

April 2020

(Sent on behalf of your ISR)

Dear FSO,

This monthly newsletter contains recent information, policy guidance, security education, and training updates. If you have any questions or recommendations for information to be included, please feel free to let us know.

WHERE TO FIND BACK ISSUES OF THE VOICE OF INDUSTRY (VOI) NEWSLETTER

Missing a few back issues of the VOI Newsletter? The VOI Newsletters, important forms, and guides may be found on the Defense Counterintelligence and Security Agency (DCSA) website, Industry Tools Page (VOIs are at the bottom of the page). For more information on personnel vetting, industrial security, or any of the other topics in the VOI, visit our website at www.dcsa.mil.

TABLE OF CONTENTS

COVID-19 NISP GUIDANCE, UPDATED APRIL 20, 2020

Please send all National Industrial Security Program (NISP) inquiries related to COVID-19 impacts to your assigned Industrial Security Representative (ISR).

Facility Clearance (FCL) Processing: FCL requests will continue to be processed. However, FCL Inquiries (Option 3 of the DCSA Knowledge Center) have been suspended until further notice. Status inquiries can be obtained by leaving a detailed voicemail message on the Knowledge Center voicemail or sending a detailed email to the Facility Clearance Branch (FCB) mailbox at dcsa.fcb@mail.mil. Please include your Facility CAGE Code and name for all status inquiries. All messages will be returned within one day.

Personnel Security: Contractors are encouraged to continue to utilize the Knowledge Center to resolve system lockouts for the Joint Personnel Adjudication System (JPAS), the Defense Information System for Security (DISS), and National Industrial Security System (NISS). Please be mindful of the menu options, which may have changed, and follow the instructions as applicable.

In conjunction with COVID-19 measures, the Department of Defense (DoD) Central Adjudications Facility (CAF) Call Center is temporarily suspending its phone service. Please submit questions/inquiries to the DoD CAF group mailbox at whs.meade.dodcaf.mbx.dodcaf-callcenter@mail.mil, and provide as much detail as possible. An agent will follow up soonest via email in the order in which the request was received.

E-QIP Reset Inquiries Change: Effective April 20, all Industry e-QIP resets will be handled by the DCSA Applicant Knowledge Center. Please call 724-738-5090 or DCSApplicantSupport@nbib.gov for assistance. For ALL other Personnel Security Clearance Inquiries, please email the Vetting Risk Operations Center (VROC) at dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil or submit a customer service request via DISS.

Employment Flexibility for Investigative Methods: Due to COVID 19 restrictions, maximum flexibility is permitted in employing alternative investigative and adjudicative methods. Such methods include virtual interviews and remote secure access to records. More information may be found here.

Industry Fingerprint Submissions for Background Investigations Guidance: Because of the COVID-19 pandemic, the Under Secretary of Defense for Intelligence and Security (USD(I&S)) provided personnel vetting guidance for the continued collection and processing of fingerprints. The USD(I&S) guidance states DoD, to the greatest extent possible, will continue to follow established guidance for vetting contractors under DoD cognizance for the NISP.

Please refer this list for fingerprint service providers supporting geographic areas across the country.

For investigation requests where the fingerprint check is completed, please submit the investigation request to VROC. The fingerprint check will result in a Special Agreement Check (SAC) investigation populated on the JPAS Person Summary Screen. The SAC investigation is valid for 120 days from the closing date.

If the fingerprint check was not completed, it is requested that the investigation request not be submitted to VROC until the fingerprints are captured and submitted to SWFT for processing.

For investigation requests that have been submitted to VROC without fingerprint submissions, VROC will hold the investigation request until the SAC is populated in JPAS.

VROC will continue to monitor the impacts of COVID 19 and the investigation submission process.

COVID-19 Personnel Reporting: There are no reporting obligations for contractors with regard to employees having COVID-19 or possibly being in contact with COVID-19 at this time.

Administrative Debriefs: Cleared contractors under DoD cognizance may, until further notice, on a case-by-case basis, conduct administrative debriefs of cleared personnel leaving employment when the employee is not physically available. The administrative debrief may be conducted via telephone or email unless the discussion of classified material is required. The Facility Security Officer (FSO) must obtain an acknowledgement from the debriefed employee for retention of records. Once debriefed, JPAS must be updated to reflect the action. For email debriefs of personnel with SAP or SCI access, follow guidance provided by the Government customer.

Refresher Training: The NISP Operating Manual (NISPOM) requires training to be conducted annually, and must be conducted once during each calendar year unless specifically identified in the training requirement or by the Government Contracting Activity (GCA). Virtual training for employees is encouraged when physical presence is not possible. Until further notice, cleared contractors may adjust scheduled NISPOM refresher training based on employee availability and status. Cleared contractors will have a plan in place to ensure that refresher training is resumed and that all overdue training is completed within 60-days of returning to normal operations. This does not preclude training requirements for personnel that remain on duty and the training is required to perform security related tasks (for example, derivative classification training that must be current for all derivative classifiers). Cleared contractor employees not in current work status (furloughed or not in pay status) should be removed from access in JPAS and as such, do not require training to be maintained until they return to work.

Security Reviews: Due to the COVID-19 National Emergency, DCSA is suspending all Enhanced Security Vulnerability Assessments (ESVAs) and on-site activities until further notice. Facilities scheduled to receive an ESVA will instead be contacted virtually by their ISR who will conduct a Continuous Monitoring Engagement. Please contact your assigned ISR with any questions.

Safeguarding: All classified information should be properly secured in accordance with NISPOM requirements and approved safeguarding procedures prior to office closure. This includes areas implementing mandatory quarantines. The contractor must contact their ISR if they encounter any issues following office closure.

Cleared contractors should also ensure that NISPOM 5-103, Perimeter Control, requirements are in place to screen material exiting spaces that hold classified material. When unclassified information systems are removed from approved spaces that hold classified information, measures should be in place to ensure that the systems do not host classified material. Contractors should coordinate with their Government customer on the removal of systems that host unclassified Government material prior to removal or where previous approval has not been provided.

Safeguarding/Closed-Area Approvals: During this time, all-new safeguarding/closed-area approval requests will require the GCA to address a compelling letter of need to DCSA. When received, the ISR is authorized to leverage virtual/remote means to validate requirements. Security safeguarding requirements must be met for consideration. If the ISR does not feel they are able to appropriately validate the safeguarding requirements (such as construction of a Closed Area) in a virtual session, it will not be approved. Virtual approval for Top Secret safeguarding is not authorized at this time.

Self-Approval Authority for Closed-Areas: If the FSO has self-approval authority, then the contractor shall continue to be responsible for inspecting and approving Closed Areas with qualification criteria. Self-approval authority does not require on-site validation from DCSA personnel. This includes approval authority above Secret. However, if the FSO does not have self-approval authority, a compelling letter of need with risk acceptance to DCSA is required for all-new Closed Area requests at the Secret or below level. This will be coordinated through virtual means by DCSA personnel. Please be advised that approval above Secret by DCSA personnel will not be authorized at this time.

Closeout Assessments: Due to the pandemic, DCSA personnel are not able to conduct on-site closeout assessments for facilities that no longer require safeguarding, and therefore cannot verify that all classified material has been appropriately disposed. Therefore, the following procedures will be followed:

- Obtain written confirmation from GCA or prime contractor that the facility no longer requires the ability to safeguard classified information, and forward that information to DCSA.
- The FSO and the Senior Management Official must provide written correspondence to DCSA that confirms that all classified material has been appropriately disposed. Supporting documentation should include destruction receipts, information management system details, etc.

End-of-Day Checks: End-of-day checks on security containers and secure areas are not waived. The contractor is responsible for ensuring classified material remains appropriately secured. If security containers are located in an open workspace (such as a hallway) or in a secure space that has been opened (such as a Closed Area), end of day checks need to be conducted. However, during the COVID-19 pandemic, if security containers are in a secure area that was **not** opened, the space does **not** need to be opened simply to conduct end-of-day checks on the container. If the office is closed and the contractor can confirm that no one entered the office space, there is **no** need for an authorized employee go in and check the containers or secure areas and perform end-of-day-checks.

DCSA Approved Closed Areas: If a DCSA-approved secure space safeguards Top Secret information, all efforts should be made to continue to leverage dual authentication while mitigating the risk of virus transmission (example: latex gloves, keypad sanitization, etc.). However, if the contractor's access cards allow for identification of whoever is entering the space, and the contractor can ensure physical control of all access cards by the respective owners, then the contractor may decide to temporarily suspend the need for a PIN. The contractor should specify a length of time for the suspension, not "until further notice" (example - 2 weeks at a time), and reevaluate circumstances at the conclusion of that time period. The contractor should also identify additional accountability requirements and checks for the access cards to manage the risk posed by removing the dual authentication. The contractor should notify their ISR that they are implementing temporary measures and keep DCSA informed of the status and any issues.

Special Access Program Facilities (SAPFs): In accordance with DoDM 5205.07-V3 Physical Security, DoD Component Special Access Program Central Offices (SAPCOs) with cognizant authority and oversight authority over SAPs grant waivers to the standards stipulated in this volume based on a risk assessment and operational requirements. DCSA does not authorize or accredit SAPFs regardless if DCSA is the cognizant security office or if there is an approved carve-out provision relieving DCSA of the industrial security oversight role. Accreditation of SAPFs is usually accomplished by the Government Program Security Officer (PSO). Approval of changes to the standards for SAPFs should be coordinated to the Cognizant Authority SAPCO through the appropriate PSO.

Transmission: Use of FedEx to transmit classified material requires prior approval from DCSA (NISPOM 5-403(e)). Additionally, DCSA has received notification of instances where FedEx is delivering packages without obtaining required signatures. If DCSA has approved a facility to use FedEx to transmit classified material and the facility has plans to do so during the COVID-19 pandemic, the facility must:

- Validate with FedEx that it will be delivered in accordance with requirements (i.e. only delivered after a signature is obtained), and
- Validate that the receiving facility is open and an appropriately cleared individual with a need-to-know is available to receive the package.

If a contractor is closing their office, they should notify their GCA(s), prime contractor(s), and ISR to pre-empt any transmission of classified information to their office.

Classified material should **not** be delivered and left unattended. Any instance of classified material being delivered or received inappropriately is considered a security violation and must be processed as such.

Authorized Information Systems: DCSA will extend all Authorizations to Operate (ATOs) expiring before April 18, 2020 for an additional 90 days. This will allow DCSA to work with Industry to ensure operations to support the warfighter and classified programs are sustained. The following guidance from the DCSA Assessment and Authorization Process Manual (DAAPM) is also provided:

Assessment and Authorization Activities (DAAPM 2.1): Security Control Assessment (SCA) activity will continue to occur. The on-site portion of the SCA activity will be delayed, deferred, or rescheduled. Documenting evidence of security and validation requirements remain unchanged; only the execution of on-site activity will change temporarily.

Audit Variances (DAAPM Section 12): During periods of system inactivity (e.g., hibernation) or when a facility plans to stop work for an extended period of time (e.g., holiday shutdowns), an audit variance may be authorized. Periods of hibernation will not exceed 180 days without Regional Authorizing Official approval. When requesting an audit variance, Industry must have a Standard Operating Procedure (SOP) in place that specifies how the system will be protected during a dormant state. The SOP will include a process for protecting the system through the use of physical security controls (e.g., seals, locks, alarms, and GSA-approved containers), technical controls (e.g., whole disk encryption, disabled accounts, and audit logs), and immediate patching/updates upon return to service. The audit variance will be authorized via the security plan (i.e., added as a supporting artifact). Industry is required to maintain a log of audit variance activities on-site. Audit variance documentation will be assessed during the ESVA and other engagement activities (e.g., Advise & Assist visits, periodic communications, etc.).

NISP AUTHORIZATION OFFICE (NAO)

NEW FEATURE IN NISP eMASS

The NAO announces a new feature in the NISP Enterprise Mission Assurance Support Service (eMASS). NISP users are now able to access the DCSA helpful documentation and job aids any time by clicking [Help] at the top of the eMASS page. The available documentation includes the DAAPM and Appendix A, NISP eMASS Industry Operation Guide, eMASS Job Aids and forms, Frequently Asked Questions, plus DAAPM forms and templates. All of the documentation is located under "Organizational Artifact Templates, SOPs, and Guides" on the eMASS Help page. Questions or concerns should be addressed to the NAO eMASS Mailbox at dcsa.quantico.dcsa.mbx.emass@mail.mil.

RELEASE OF NAO FREQUENTLY ASKED QUESTIONS 2020

The NAO recently released an update to the Frequently Asked Questions (FAQs). The 2020 update provides answers to the most frequently asked questions regarding Risk Management Framework (RMF) Assessment and Authorization activities and eMASS navigation. The NAO FAQs 2020 are posted towards the bottom of this page. Refer to DAAPM Version 2.1 and NISP eMASS Industry Operation Guide Version 1.1 for additional clarification. Questions of a specific nature should be addressed to the assigned Information Systems Security Professional (ISSP) or visit the DCSA Website.

FEDERAL INFORMATION SYSTEMS REMINDER

A Federal Information System (FIS) is owned and authorized by a United States Federal Agency. The operation of an FIS in a cleared contractor facility under DCSA cognizance may only occur if a formal agreement between the Information Owner and the cleared contractor has been established. The criteria detailed in DAAPM Section 9.8 must be met when a formal agreement is absent. In addition to meeting the conditions in the DAAPM, the FIS is required to directly support a program or contract already functioning in a formally-approved area under DCSA security oversight. DCSA will not approve a Closed Area for the sole purpose of safeguarding an FIS. Questions of a specific nature should be addressed to the assigned ISSP or visit the DCSA Website.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

EMAIL TO CAPTURE SYSTEM ENHANCEMENTS

Just a reminder, DCSA has established a mailbox to capture system enhancement requests from Industry and Government stakeholders. Please submit your system enhancements to DCSA.NISSRequirements@mail.mil. For technical issues with NISS, continue to contact the DCSA Knowledge Center at 888-282-7682, select Option 2 for system assistance and Option 2 again for NISS.

INDUSTRIAL FACILITY PROFILE UPDATES

The Full Operational Capability (FOC) for Industrial Facility Profile Updates will give Industry the ability to suggest updates to information on the Safeguarding tab and the FOCI/International tab. FOC is currently in the test phase of development and is on schedule to be deployed mid- to late-summer 2020.

VETTING RISK OPERATIONS CENTER (VROC)

INDUSTRY DISS AUTOMATED PROVISIONING INITIATIVE

From May 4 to 27, the Defense Manpower Data Center (DMDC) will conduct automated provisioning of DISS Joint Verification System (JVS) accounts for Industry Security Management Offices. This is one of the major steps in fully deploying DISS as the JPAS replacement for the DoD. Eligible recipients will receive two email notifications: (1) user provisioning instructions and (2) credentials to access the DISS JVS application. For those who wish to manually request a DISS account, please follow the PSSAR Industry instructions on the DMDC website or contact the Industry Provisioning Team at DCSA.dcsa-northern.dcsa-dvd.mbx.provisioning@mail.mil.

CONTINUOUS EVALUATION (CE) ENROLLMENT HISTORY IN DISS

The DoD CE enrollment history records are now visible in DISS. The history will display the CE enrollment reason Code and the date of the enrollment or dis-enrollment into the DoD's CE program. Any DISS user with general access will be able to see this information on the subject's summary page. For specific instructions, click here and go to Question 43.

DQI - OVERDUE PERIODIC REINVESTIGATIONS

The Defense Manpower and Data Center will conduct a Data Quality Initiative (DQI) in the JPAS in mid-May to address subjects with Overdue Periodic Reinvestigations. In mid-May, impacted FSOs will receive a JPAS message with specific instructions on how to remedy the subject's record.

INDUSTRY JPAS RRU/NDA UPDATE

On June 1, DMDC will disable the Research, Recertify and Update (RRU) functionalities in JPAS. All Customer Service Requests (CSRs) to include RRU requests and Non-Disclosure Agreements (NDAs) (SF312s) must be submitted via the DISS application. For instructions on how to complete CSR/NDA actions, please reference the user manual, under the Help link on the DISS JVS application or search "DISS Tips and Tricks" on the DCSA website. To avoid any disruption of service, it is imperative to obtain a DISS account to ensure a seamless transition from JPAS to DISS. For additional questions or concerns, please contact VROC at dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil.

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

The DCSA NAESOC oversees and services "Access Elsewhere" facilities in the NISP. It provides optimal security oversight scaled to the specific requirements of non-possessor facilities.

The NAESOC continues on its path of growth and support for the security of industry partners. Our customer oversight base as of mid-April is currently 3,305 facilities as we have completed approximately 95% of the Field Office transfers identified at this phase. All newly assigned facilities will receive a "Welcome Letter" via email including a "Frequently Asked Questions" introduction and update. Facilities can also see they have been assigned to the NAESOC by reviewing the Field Office assignment within NISS.

The NAESOC continues to refine and improve tailored oversight and educational processes to ensure the successful performance of its mission. In light of the current COVID 19 National Emergency, the NAESOC Help Desk is providing a modified workflow to best support its customers' questions and reporting needs. For all phone calls to the NAESOC Help Desk, customers may leave a detailed voicemail message including your name, phone number, facility name and CAGE Code, and a brief summary of the reason for your call. Alternatively, you may send an email to DCSA.NAESOC.generalmailbox@mail.mil or send a message through NISS Messenger. Voice messages will be returned within one business day. In addition, all in-person events are postponed until further notice.

Use NISS for:

- FCL Package – Report all Changed Conditions
- DD Form 441s (FEB 2020) – Now updated to accept electronic signatures
- Messenger Box – Report all Security Violations
- Facility Profile Update Requests – Information that can be edited by Industry users includes, but is not limited to new contracts, program assets, and Key Management Personnel contact information.

You can reach the NAESOC team in the following ways:

- Phone 888-282-7682 and select Option 7
- Email dcsa.naesoc.generalmailbox@mail.mil (Subject Line: Facility Name & CAGE Code)
- Mail written correspondence to NAESOC Field Office, PO Box 644 Hanover, MD 21076

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

SPĒD CERTIFICATION PROGRAM UPDATES

On June 1, the Security Professional Education Development (SPēD) Certification Program will migrate account creation and profile management from Security Training, Education, and Professionalization (STEPP) to My SPēD Certification (MSC).

In addition, beginning May 14, the SPēD participation check box option located on your STEPP profile will be removed. MSC will be the only location for new and existing account creations. MSC has a planned scheduled maintenance event and will not be available from 12 a.m. EST on Saturday, May 16, through 12 a.m. EST on Monday, June 1.

The SPēD Certification Program is also in the process of making updates to the Certification Renewal Form (CRF). If you have a CRF pending submission, submit your completed CRF prior to May 15 to prevent losing saved information. Starting June 1, you will be required to submit a new CRF for your SPēD certification renewal.

Current MSC account users: The migration will not affect profiles already created in MSC. You will be required to update your profile and complete several new data fields of information upon log in. Starting June 1, records will only be available in MSC.

Non-CAC holders will be required to submit a manual account creation form to regain/gain access to your MSC account. The manual account creation form can be found on the MSC login page above the DoD ID field or by contacting your Component Service Representative after June 1. You will be notified by the SPēD Program Management Office within 72 duty hours when your account is approved.

CDSE will send reminders and updates as necessary.

UPCOMING KNOW YOUR CDSE SPEAKER SERIES

CDSE invites you to participate in our upcoming Speaker Series:

- Know your CDSE: Counterintelligence
  Thursday, May 14, 2020
  12:00 p.m. - 12:30 p.m. ET
  Join this live, interactive 30-minute event to learn about CDSE's many Counterintelligence (CI) awareness courses, performance support tools, and resources available to enhance your CI Awareness Program.
- Know Your CDSE: Certification and Education
  Thursday, June 4, 2020
  12:00 p.m. - 1:00 p.m. ET
  Join this live, interactive one hour event to learn about our Certification and Education programs.

Register for all Speaker Series at CDSE Webinars.

NEW SAP SECURITY AWARENESS GAME

CDSE has just released "SAP Stacks," a new security awareness game integrating commonly used Special Access Program terms and definitions. The SAP Stacks word game can be found here.

NEW INDUSTRIAL SECURITY WORD SEARCHES

CDSE has just released three more word searches! These word search puzzles are not only fun but will give you a clear understanding of the meaning of the terms you will encounter throughout the NISP. Learning these terms will help you understand the "why" behind your NISPOM requirements. Besides, who doesn't enjoy a good word search puzzle? Visit CDSE Security Awareness Games to check them out!

NEW COUNTER PROLIFERATION COURSE COMING SOON

Counter Proliferation, or "CP," is a growing, emerging discipline in the national security community. CP represents the actions taken to defeat the threat and/or use of weapons of mass destruction against the United States and our military forces, friends, and allies.

This summer, CDSE will release a new 45-minute eLearning course for FSOs and security managers to learn the basics of CP and to be able to apply export control safeguards to determine if an export is allowed. The course is designed to help students define and describe CP, recognize partnering organizations, understand policy guidance, demonstrate an understanding of export permission guidelines, and explain steps used to prevent and report export control violations.

DCSA ACCESS FEATURES CDSE 10 YEAR ANNIVERSARY ARTICLE

"CDSE celebrates a decade of achievement, helping to secure the nation."

CDSE is featured in the recently released DCSA Access magazine, highlighting CDSE's 10-year anniversary. For over 10 years, CDSE has worked to develop security skills, increase security knowledge, and promote security awareness in the DoD and cleared industry workforces. We've educated, trained, and certified millions of personnel entrusted with protecting national security.

To learn more about the achievements and evolution of CDSE, see DCSA Access Volume 9 Issue 2 to read the article, "CDSE Works to Professionalize the Security Workforce."

NEW INSIDER THREAT POSTER

In April, we released a new Insider Threat poster, "Resilience Pathways." This poster is part of an ongoing series on Resilience, which is CDSE's Insider Threat theme for 2020. Check out this and other posters at Insider Threat Security Posters.

INSIDER THREAT TOOLKIT

We added a number of new resources to the Insider Threat toolkit under the Research tab, including PERSEREC's inaugural graphic novel and new issues of their "Bottom Line Up Front" newsletter. Check out the updates and the content in the other tabs, as well.

INSIDER THREAT JOB AID

We updated and refreshed the Insider Threat glossary of terms, adding new definitions and making the format more user friendly. Check out the updated job aid here.

NATIONAL SUPPLY CHAIN INTEGRITY MONTH

During the month of April, CDSE highlighted information to raise awareness about supply chain threats and resources to help mitigate the risk. National Supply Chain Integrity Month may have come to an end but foreign intelligence entities and other adversaries will continue to attempt to compromise our Government and industry supply chains. Employing strategies to mitigate the risk to vulnerable supply chains is a year round mission for trusted suppliers and vendors facing infiltration that targets equipment, systems, and information used daily by the Government, businesses, and individuals.

Continue to access the following supply chain integrity resources of CDSE and the National Counterintelligence and Security Center (NCSC) to help our country avoid paying a steep price in lost innovation, jobs, economic advantage, and reduced U.S. military strength:

- CDSE Counterintelligence Toolkit: Supply Chain Risk Management
- CDSE Counterintelligence Toolkit: Deliver Uncompromised
- NCSC - Supply Chain Risk Management
- Archived CDSE April Supply Chain Integrity Speaker Series (under CI):
  - Counterintelligence, the Supply Chain, and You
  - Supply Chain Resiliency

NEW NISS JOB AID AND FSO CURRICULA UPDATE

On May 6, the NISS External User Training IS127.16 eLearning course will no longer be available in STEPP. This course will be removed from the FSO Orientation for Non-Possessing Facilities IS020.CU and FSO Program Management for Possessing Facilities IS030.CU curricula.

The new NISS External User Guide Job Aid, released by DCSA, is available now. You can find it on the Facility Clearance page of the FSO Toolkit.

APRIL PULSE: CDSE SECURITY AWARENESS NEWSLETTER

In April, we released the fourth in a series of monthly security awareness newsletters called CDSE Pulse. The April newsletter featured National Supply Chain Integrity Month content. Check out all the newsletters in the DCSA Electronic Reading Room or subscribe/update your current subscription and get the newsletter sent directly to your inbox by submitting your email address at CDSE News.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE