Foreign Influence and Research Security: The Challenges Continue

August 18, 2020

Moderator:

Robert Hardy, Director of Research Security & Intellectual Property (COGR)

Panelists:

Stephen Binkley, Principal Deputy Director, Office of Science, Department of Energy

Lizbet Boroughs, Associate Vice President for Federal Relations, Association for American Universities (AAU)

Michael Corn, Chief Information Security Officer, University of California, San Diego and Co-Chair, Educause Higher Education Information Security Council (HEISC)

Elizabeth Peloso, Associate Vice Provost and Assoc. Vice President for Research Services, University of Pennsylvania

Hanan Saab, Asst. Vice President for Federal Relations, (AAU)

COGR
Council On Governmental Relations

Today's Topics

- DOE Update
- NDAA & Congressional Developments
- CMMC & Cybersecurity
- Section 117 Update
- Immigration Update
- Q&A

COGR
Council On Governmental Relations

DOE Update

Stephen Binkley, Principal Deputy Director, Office of Science, Department of Energy

COGR
Council On Governmental Relations

NDAA & Congressional Developments

Hanan Saab, Asst. Vice President for Federal Relations, (AAU)

SEC. 1746. SECURING AMERICAN SCIENCE AND TECHNOLOGY.

(a) INTERAGENCY WORKING GROUP.—

(1) IN GENERAL.—The Director of the Office of Science and Technology Policy, acting through the National Science and Technology Council, in consultation with the National Security Advisor, shall establish or designate an interagency working group to coordinate activities to protect federally funded research and development from foreign interference, cyber attacks, theft, or espionage and to develop common definitions and best practices for Federal science agencies and grantees, while accounting for the importance of the open exchange of ideas and international talent required for scientific progress and American leadership in science and technology.

(2) MEMBERSHIP.—

(A) IN GENERAL.—The working group shall include at least one representative of—

(i) the National Science Foundation;

(ii) the Department of Energy;

(iii) the National Aeronautics and Space Administration;

(iv) the Department of Commerce;

(v) the Department of Health and Human Services;

(vi) the Department of Defense;

(vii) the Department of Agriculture;

(viii) the Department of Education;

(ix) the Department of State;

(x) the Department of the Treasury;

(xi) the Department of Justice;

(xii) the Department of Homeland Security;

(xiii) the Central Intelligence Agency

FY 21 National Defense Authorization Act

Key Provisions of Interest

Sec. 281 National Security Innovation Pathways

Sec. 1763 Online and Distance Education Classes

Sec. 279 Traineeships for American Leaders to Excel in National Technology and Science (TALENTS)

Sec. 229 Disclosure of Foreign Funding Sources in Applications for Federal Research Awards

Sec. 6282 Academic Liaison to Protect Against Emerging Threats

Sec. 228 Measures to Address Foreign Talent Programs

Sec. 1264 Enhanced Information Sharing Requirements for Basic Research

Sec. 830B Prohibition on Procurement or Operation of Foreign-Made Unmanned Aircraft Systems

COGR
Council On Governmental Relations

Other Congressional Activity

Recent Bill Introductions & Legislative Updates

S. 3997 Safeguarding American Innovation Act

S. 4370 Stop Theft of Intellectual Property Act

H.R. 7842 INFLUENCE Act

S. 939 CONFUCIUS Act

S. 3837 COVID-19 Vaccine Protection Act

House GOP China Task Force

COGR
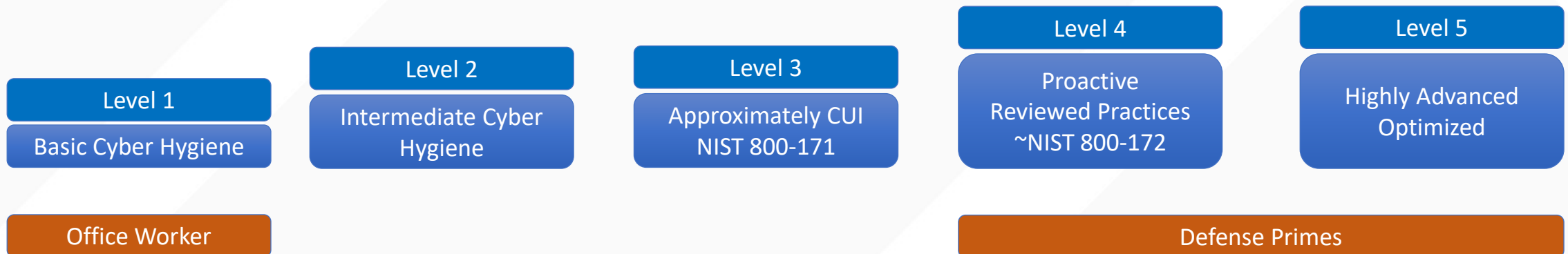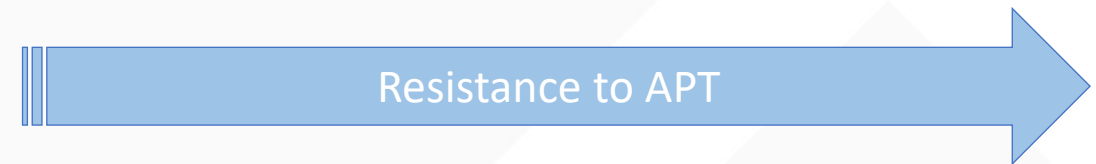Council On Governmental Relations

CMMC & Cybersecurity

Michael Corn, Chief Information Security Officer, University of California, San Diego and Co-Chair, Educause Higher Education Information Security Council (HEISC)
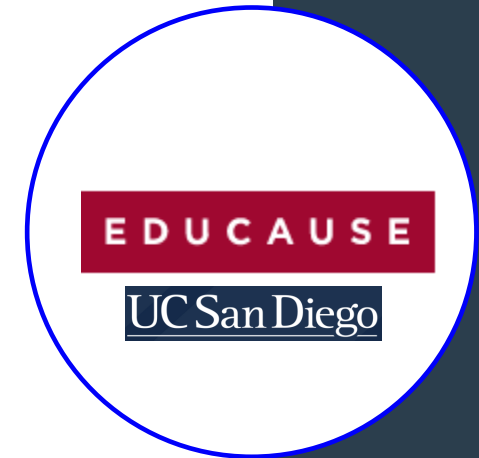
CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) IN A NUTSHELL

- Five tier system of security and IT practices

- Largely based on NIST 800-53

- Each tier represents an increasing level of maturity of practices

- For security professionals the items in each tier are familiar

https://xkcd.com/927/

Resistance to APT

Level 1	Level 2	Level 3	Level 4	Level 5
Basic Cyber Hygiene	Intermediate Cyber Hygiene	Approximately CUI NIST 800-171	Proactive Reviewed Practices ~NIST 800-172	Highly Advanced Optimized

Office Worker	Defense Primes

COGR
Council On Governmental Relations

CMM <u>CERTIFICATION</u>

- Requires each environment to be <u>pre-certified</u> prior to responding to a solicitation

- Certification audit performed by an assessor who is trained and certified by the CMMC-AB (accreditation body) <u>https://www.cmmcab.org/</u>

- Certification is lasts for three years

- CMMC program has suggested a Level 1 <u>institutional certification</u> may be required

- <u>Only DoD contracts</u> are in scope initially
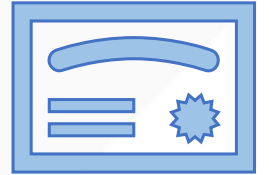
Timeline

- Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 is undergoing a rule change to include CMMC (expected completion October 2020)

- CMMC expected in contracts starting November 2020 and continuing through 2026 for comprehensive implementation

- DoD expects 7500 organizations to achieve certification in 2021 (~20 / day)

COGR
Council On Governmental Relations

WHAT WILL CMMC MEAN FOR YOUR INSTITUTION

- A failure to address could result in a complete loss of DoD funding in the next decade

- An institutional certification could cost 7+ figures to achieve

- Basic research exemption only at the discussion phase

- Contract flow down could result in Level 4 & 5 obligations

- CMMC enclaves could take 6 months to 1 year to bring into compliance

- Certifying labs (or ships) in situ will be very challenging and has not be addressed by CMMC standards explicitly

CMMC is Research Issue

CMMC is operationalized by infosec

Research culture is one of autonomy

CMMC is blind to COVID

COGR
Council On Governmental Relations

TACKLING THE DIVERSE IT ENVIRONMENTS: INTERNAL SELF-CERTIFICATION

Define and publish internally a baseline standard based around CMMC L1 aka "Cybersecurity Baseline for Research"

- Ensure and encourages common security controls (e.g., anti-malware software, regular patching) and record-keeping are deployed

- Provides visibility for early detection of attacks and compromises which is critical for response and remediation

- Education of IT staff is critical! Emphasize practice and not 'controls' or 'security'

- Security, research IT / facilitators / divisional leaders can assist labs with security guidance and baseline implementation

Require labs to self-certify compliance with the UC San Diego Baseline for Research

- Ensures

  - Labs and distributed IT assets are identified with local accountability identified

  - Local IT teams with labs, working with central IT, can improve their cybersecurity position

- Begins shifting the culture around pro-active cybersecurity management, periodic assessment and continuous improvement and significantly prepares UCSD for Federal imposition of CMMC or similar standards

- Biennial process

- Program overview and introduction at https://assure.ucsd.edu

COGR
Council On Governmental Relations

Section 117 Update

Elizabeth Peloso, Associate Vice Provost and Assoc. Vice President for Research Services, University of Pennsylvania

COGR
Council On Governmental Relations

Department of Education Section 117 reporting

-New reporting requirements in 2020 include

    Required identification of donors

    Expanded definition of institutions

    Expanded definitions and information requirements for foreign sources

    Identification of intermediaries

    Detailed information on foreign contract restrictions

-New reporting portal for 2020 (first use for July 31 reporting deadline)

    Limited functionality

    No ability to correct a submitted record

-Still no defined process to correct/amend past reporting periods

-COGR is planning to reach out to the department of Education on these issues

COGR
Council On Governmental Relations

Immigration Update

Lizbet Boroughs, Associate Vice President for Federal Relations, Association for American Universities (AAU)
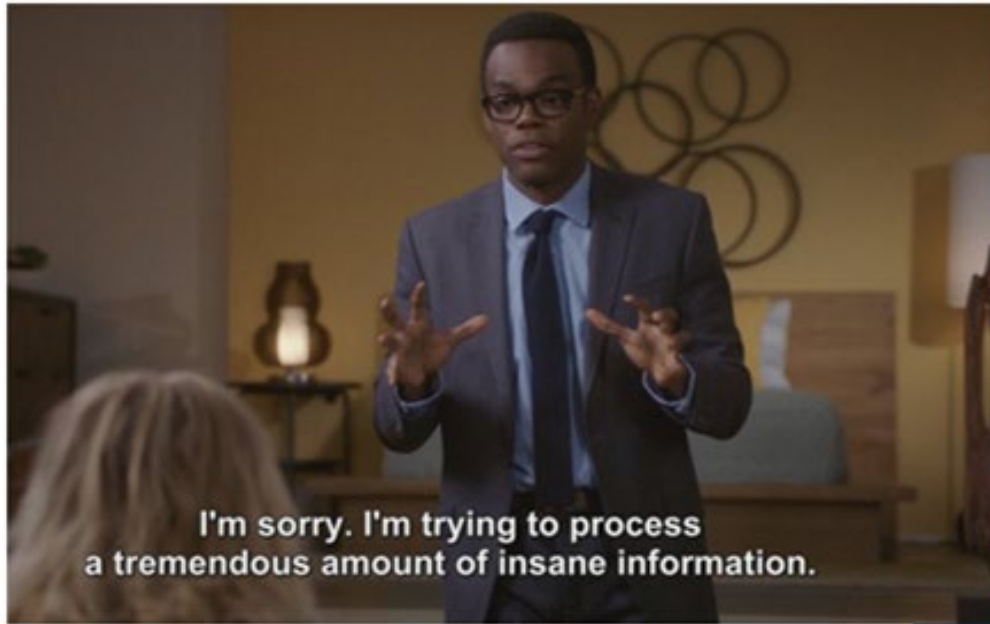
Policy changes from administration

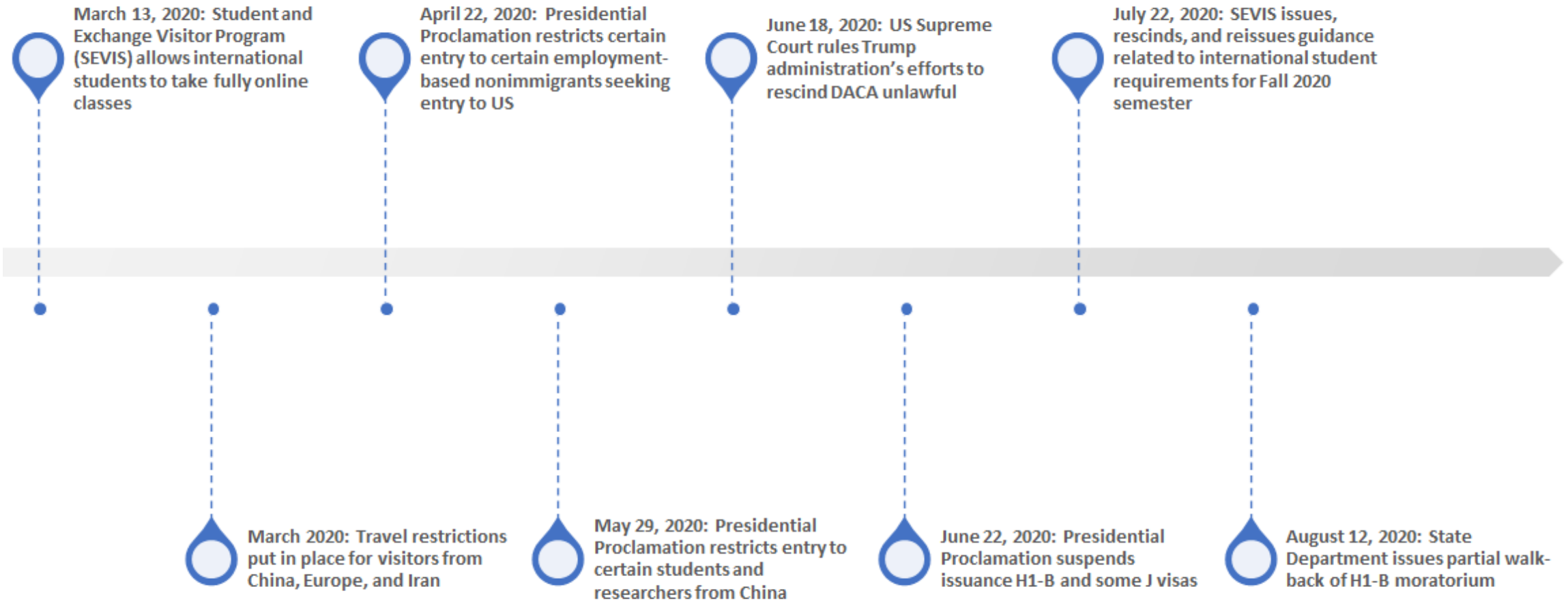# Three "buckets" facing international students and scholars

OBTAINING VISAS FROM STATE DEPARTMENT

OBTAINING ENTRY INTO THE US FROM CUSTOMS AND BORDER PROTECTION

OBTAINING EMPLOYMENT AUTHORIZATION FROM USCIS

COGR
Council On Governmental Relations

March 13, 2020: Student and Exchange Visitor Program (SEVIS) allows international students to take fully online classes

April 22, 2020: Presidential Proclamation restricts certain entry to certain employment-based nonimmigrants seeking entry to US

June 18, 2020: US Supreme Court rules Trump administration's efforts to rescind DACA unlawful

July 22, 2020: SEVIS issues, rescinds, and reissues guidance related to international student requirements for Fall 2020 semester

March 2020: Travel restrictions put in place for visitors from China, Europe, and Iran

May 29, 2020: Presidential Proclamation restricts entry to certain students and researchers from China

June 22, 2020: Presidential Proclamation suspends issuance H1-B and some J visas

August 12, 2020: State Department issues partial walk-back of H1-B moratorium

COGR
Council On Governmental Relations

Litigation

- June 22 - skilled worker litigation filed

- July 6 order on international students and on-line learning

- SCOTUS decision on DACA recission

- September 11 hearing on high-skilled restrictions

COGR
Council On Governmental Relations

AAU Forecast

Continued guidance, rules and Executive Orders

Litigation, rather than legislation

Security concerns conflated with economy

4

COGR
Council On Governmental Relations

Q & A

Thank You

Visit us at www.cogr.edu

COGR
Council On Governmental Relations