# Research Security and Intellectual Property Committee

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patrick Schlesinger (Chair)</td>
<td>University of California, Berkeley</td>
</tr>
<tr>
<td>Alexandra Albinak</td>
<td>Johns Hopkins University</td>
</tr>
<tr>
<td>Cindy Kiel</td>
<td>University of California, Davis</td>
</tr>
<tr>
<td>Michael Moore</td>
<td>Northwestern University</td>
</tr>
<tr>
<td>Dan Nordquist</td>
<td>Washington State University</td>
</tr>
<tr>
<td>Elizabeth Peloso</td>
<td>University of Pennsylvania</td>
</tr>
<tr>
<td>Jennifer Ponting</td>
<td>University of Chicago</td>
</tr>
<tr>
<td>John Ritter</td>
<td>Princeton University</td>
</tr>
<tr>
<td>Janna Tom</td>
<td>University of California</td>
</tr>
<tr>
<td>David Winwood</td>
<td>Louisiana State University</td>
</tr>
<tr>
<td>Kevin Wozniak</td>
<td>Georgia Institute of Technology</td>
</tr>
<tr>
<td>Robert Hardy</td>
<td>Director, COGR</td>
</tr>
</tbody>
</table>
NIST Update - iEdison

- **Background**
  - NIH legacy system
  - NIH: “iEdison makes it easy to learn about the law and its regulations and report an invention or patent funded by any of the agencies listed”

- **Rebuild**
  - RFI for redesign of system from ground up at NISH

- **Next steps**
  - Received many comments and will form stakeholder groups
  - Webinar in April
  - Award in November 2020
  - Operational system in 2022
Bayh-Dole at 40

Rulemaking

- No legislative fixes recommended
- More in the nature of “housekeeping” than restructuring
- To be sent to OMB in March, NPRM in April
- Removing explanatory material from existing regulation
DOE Order 142.3A

- Unclassified foreign visits and assignments
- Exemption removed
  - Applied to research under grants performed at institutions of higher education where results are published
  - Performance of such research **not** considered “access to DOE sites, information, technology, equipment, programs, or personnel”
- FN information to be provided for DOE review
- DOE secretary or designee must approve participation of individuals from T-4 countries
- DOE HQ vs. DOE contracting officers
DOD Cybersecurity Maturity Model Certification (31 Jan 2020)

- Unified cybersecurity standard for future acquisitions

CMMC Model v1.0: Number of Practices and Processes Introduced at each Level

<table>
<thead>
<tr>
<th>CMMC Level</th>
<th>Practices</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>17</td>
<td>-</td>
</tr>
<tr>
<td>Level 2</td>
<td>55</td>
<td>2</td>
</tr>
<tr>
<td>Level 3</td>
<td>58</td>
<td>1</td>
</tr>
<tr>
<td>Level 4</td>
<td>26</td>
<td>1</td>
</tr>
<tr>
<td>Level 5</td>
<td>15</td>
<td>1</td>
</tr>
</tbody>
</table>
CMMC

**LEVEL 1**
**BASIC CYBER HYGIENE**
- 17 PRACTICES
- Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

**LEVEL 2**
**INTERMEDIATE CYBER HYGIENE**
- 72 PRACTICES
- Comply with the FAR
- Includes a select subset of 48 practices from the NIST SP 800-171 r1
- Includes an additional 7 practices to support intermediate cyber hygiene

**LEVEL 3**
**GOOD CYBER HYGIENE**
- 156 PRACTICES
- Comply with the FAR
- Includes a select subset of 11 practices from Draft NIST SP 800-171B
- Includes an additional 20 practices to support good cyber hygiene

**LEVEL 4**
**PROACTIVE**
- 171 PRACTICES
- Comply with the FAR
- Includes a select subset of 4 practices from NIST SP 800-171 r1
- Includes a select subset of 11 practices from Draft NIST SP 800-171B
- Includes an additional 15 practices to demonstrate a proactive cybersecurity program

**LEVEL 5**
**ADVANCED / PROGRESSIVE**
- 171 PRACTICES
- Comply with the FAR
- Includes all practices from NIST SP 800-171 r1
- Includes a select subset of 4 practices from Draft NIST SP 800-171B
- Includes an additional 11 practices to demonstrate an advanced cybersecurity program
FAR 52.204-21

- (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- (iii) Verify and control/limit connections to and use of external information systems.
- (iv) Control information posted or processed on publicly accessible information systems.
- (v) Identify information system users, processes acting on behalf of users, or devices.
- (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
- (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
- (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- (xii) Identify, report, and correct information and information system flaws in a timely manner.
- (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
- (xiv) Update malicious code protection mechanisms when new releases are available.
- (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
CMMC Roll-out

- Applied through 7012 clause
- Phased approach
  - Small number of prime contractors - 10 in the first years
  - But could show up in subaward
- Third-party audit/certification
- Costs
  - DOD: Should be minimal for level I ~ $5K
- Certify enclave/small number of labs
- Procedures, Guidance & Information (PGI) document needed for fundamental research?
- More information
  - COGR updates
  - AUECO Conference April 28-29, 2020 – University of Pennsylvania
Huawei Equipment Restrictions

- **NDAA FY19**
  - Manufacturers
    - Telecommunications – Huawei, ZTE
    - Telecom in public safety context – Hytera, Hangzhou Hikvision, Dahua
  - Prohibition on sale of defined equipment to USG (2019)
  - Prohibition on use of defined equipment by contractor, not in the context of a particular contract (Aug. 2020)
- “Substantial or essential part” of system
- Scan networks and replace effected equipment
- Could have components within larger pieces of equipment