



State of Industrial Control System Cybersecurity Training Opportunity

Informational Webinar / Objective Strategic Session (IW/OSS)

Scan the QR code and visit the
TechWerx website to learn
more about this Opportunity



Office of Cybersecurity, Energy
Security, and Emergency Response



TechWerx

A DOE Innovation Hub

Connecting visionaries, researchers, industry and energy leaders with the opportunities and experts to build the ecosystem, technologies, workforce and infrastructure to enable an equitable and resilient energy transition.

Scan the QR code and visit the TechWerx website to learn more about this Opportunity



Office of Cybersecurity, Energy Security, and Emergency Response (CESER)



Fania Barwick
Implementation
Manager



Cynthia Hsu
Cybersecurity
Program
Manager



Kate McGrath
AAAS Science
& Technology
Policy Fellow



Steve Lindaas
AAAS Science
& Technology
Policy Fellow



China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks.

If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces.

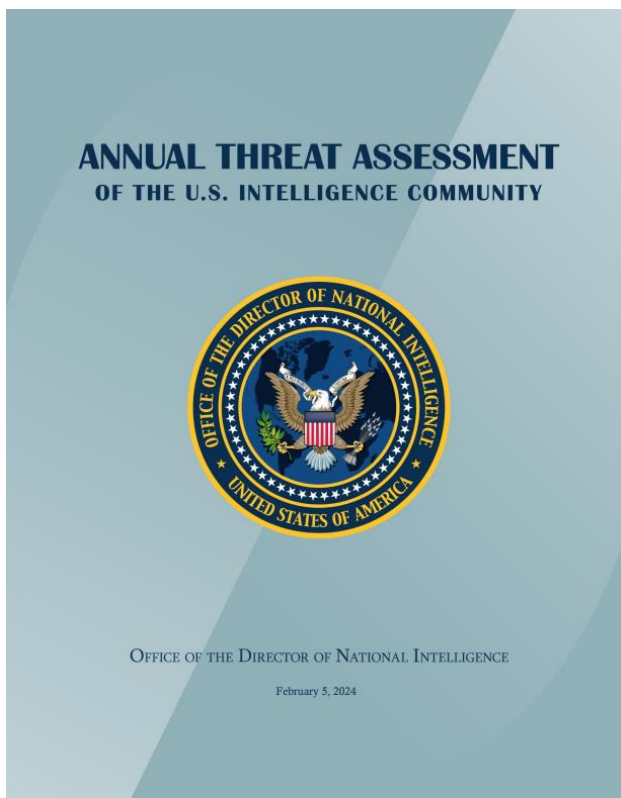


THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE'S
2024 ANNUAL THREAT ASSESSMENT

[ATA-2024-Unclassified-Report.pdf](#)

<https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china>

ODNI Annual Threat Assessment



[ATA-2024-Unclassified-Report.pdf \(dni.gov\)](#)

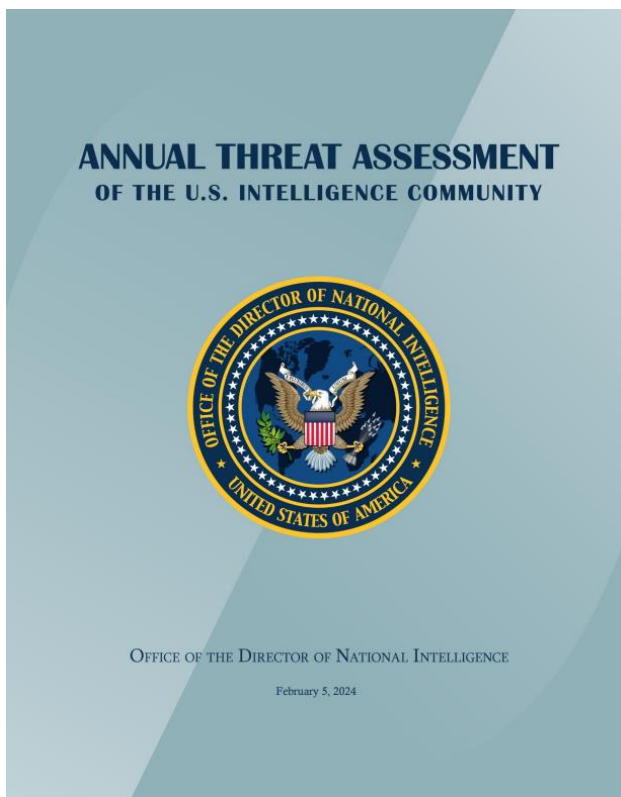
Nation-State Cyber Actors

- [China Cyber Threat Overview and Advisories](#)
- [Russia Cyber Threat Overview and Advisories](#)
- [North Korea Cyber Threat Overview and Advisories](#)
- [Iran Cyber Threat Overview and Advisories](#)



[ATA-2024-Unclassified-Report.pdf](#)
<https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china>

ODNI Annual Threat Assessment



[ATA-2024-Unclassified-Report.pdf \(dni.gov\)](#)

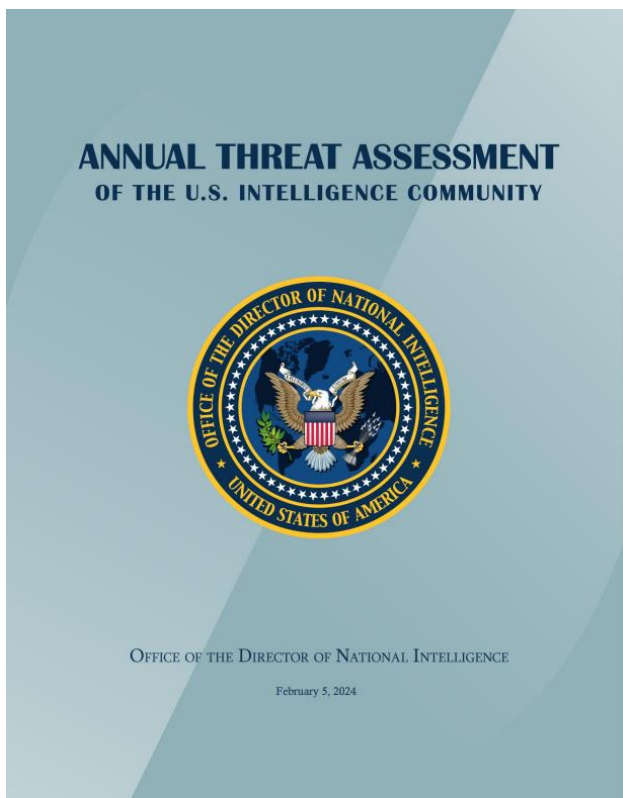
Nation-State Cyber Actors

- [China Cyber Threat Overview and Advisories](#)
- [Russia Cyber Threat Overview and Advisories](#)
- [North Korea Cyber Threat Overview and Advisories](#)
- [Iran Cyber Threat Overview and Advisories](#)



[ATA-2024-Unclassified-Report.pdf](#)
<https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china>

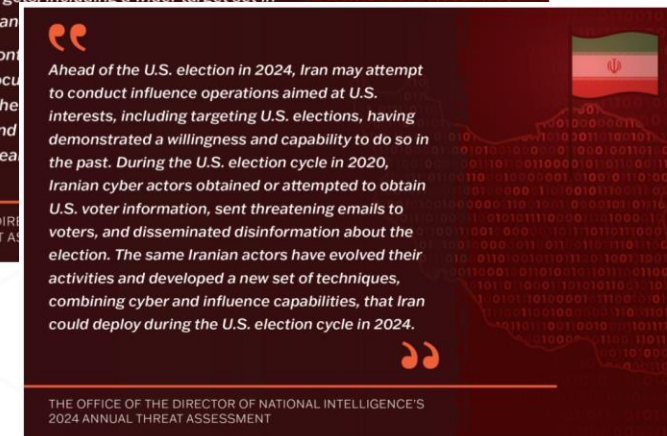
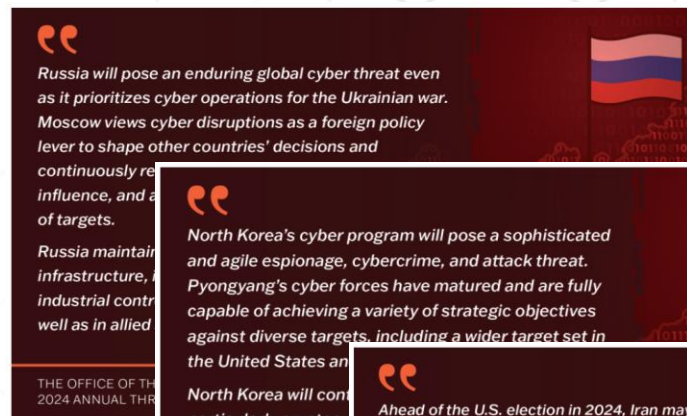
ODNI Annual Threat Assessment



[ATA-2024-Unclassified-Report.pdf \(dni.gov\)](#)

Nation-State Cyber Actors

- [China Cyber Threat Overview and Advisories](#)
- [Russia Cyber Threat Overview and Advisories](#)
- [North Korea Cyber Threat Overview and Advisories](#)
- [Iran Cyber Threat Overview and Advisories](#)



[ATA-2024-Unclassified-Report.pdf](#)
<https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china>

CESER advances our national security mission through:

- **Risk Assessment** – Identifying, analyzing, and prioritizing risks to the energy sector.
- **Risk Mitigation** – Developing policies, tools, and technologies and providing technical assistance to mitigate risks to the energy sector.
- **Sector collaboration** – Strengthening the security of U.S. energy systems through enhanced public and private sector collaboration.
- **Preparedness and Response** – Facilitating energy sector preparedness, response, and restoration efforts in collaboration with other Federal agencies, the private sector, and state, local, tribal, and territorial communities and international partners.
- **Energy Supply** – Mitigating the impacts of energy supply disruptions on American businesses and consumers.

Cybersecurity Workforce

- Increase the cybersecurity capabilities of the incumbent energy sector workforce
- Increase the pool of potential employees equipped with the appropriate cybersecurity knowledge, skills, and abilities (KSAs) to work in the energy sector



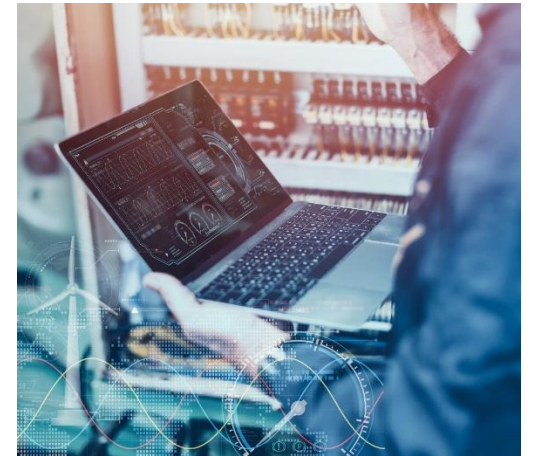
ICS/OT Cybersecurity in Energy

- Industrial control systems (ICS) and operational technology (OT) cybersecurity
- Technical knowledge and skills in cybersecurity, and in energy sector operational systems and engineering



ICS Cybersecurity Workforce Issues & Challenges

- Wide range of job roles, job titles, tasks, and skills → difficult to standardize
- Relatively new profession – limited labor and employment infrastructures that recognize ICS cybersecurity job roles and tasks



ICS Cybersecurity Workforce Issues & Challenges

- Wide range of job roles, job titles, tasks, and skills → difficult to standardize
- Relatively new profession – limited labor and employment infrastructures that recognize ICS cybersecurity job roles and tasks
- Dramatic IT cyber workforce shortages reported, unclear status of ICS cyber workforce in energy
- Entry level job descriptions not well aligned with the entry level workforce KSAs
- ICS cybersecurity responsibilities often subsumed under more common job roles



Overview: Purpose

- Support market research to understand the **current and future landscape and needs of the energy sector's ICS/OT cybersecurity workforce.**
- Inform the **development of a strategic plan** for enhancing the energy sector's cybersecurity workforce by identifying areas for future investment.

Overview: Objective & Project Details

- Seeking proposals from performer(s) with knowledge of:
 - ICS/OT cybersecurity workforce training and development programs, and/or
 - The energy sector workforce and pipeline for ICS/OT cybersecurity professionals.
- Approximately \$160k will be available to fund 1-2 awards.
- Projects are expected to be 6 months in length, with the ability to add a one-time 3-month no cost extension.

Overview: Efforts

This Opportunity will fund **three related efforts**:

1. State of ICS/OT Cybersecurity Workforce Development and Training
2. Energy Sector ICS/OT Workforce Needs and Pipeline
3. ICS/OT Cybersecurity Workforce and Strategic Plan

For additional details:



Effort 1: State of ICS/OT Cybersecurity Workforce Development and Training

Identifying existing workforce development mechanisms that improve an employee's ICS/OT cybersecurity skills and abilities, for example:

- Internships, apprenticeships, cybersecurity clinics, and other skills-based on-the-job training programs;
- Competitions, cyber ranges, boot camps, etc.;
- Training courses, degrees, and/or certifications offered by academic, nonprofit, for-profit, and vendor/original equipment manufacturers; and
- Other types of workforce development methods in use for the energy sector or that could be adapted for use in a workforce development program for the energy sector.

Effort 1: Check Data Categories You Will Collect

- ❑ Providers of commercially available ICS/OT cybersecurity workforce development and training;
- ❑ Academic programs that include ICS/OT cybersecurity;
- ❑ Two-year academic programs and those located in rural and/or tribal communities;
- ❑ Not-for-profit organizations and programs providing ICS/OT cybersecurity workforce development and training;
- ❑ Original equipment manufacturers that provide ICS/OT cybersecurity training associated with their products/services;
- ❑ Security vendors and service providers that provide ICS/OT cybersecurity workforce development and training;
- ❑ Government agencies (military and civilian) that provide ICS/OT cybersecurity workforce development and training, including but not limited to DOE, FBI, DHS/CISA, DoD (e.g., National Guard), etc.;
- ❑ Federally Funded Research and Development Centers (FFRDCs) and national laboratories that provide ICS/OT cybersecurity workforce development and training;
- ❑ Other public sector entities, e.g., non-energy utilities, manufacturing, libraries, etc., that provide ICS/OT cybersecurity workforce development and training;
- ❑ Other private sector entities, e.g., trade organizations, energy markets, manufacturing, non-energy utilities, insurance companies, financial companies, etc., that provide ICS/OT cybersecurity workforce development and training.

Effort 2: Energy Sector ICS/OT Cybersecurity Workforce Needs and Pipeline

Collect and analyzed data for small (<50 employees), medium (50-300 employees), and large (>300 employees) organizations addressing questions including but not limited to:

- Where does the energy sector go to hire ICS/OT cybersecurity talent?
- When ICS/OT cybersecurity employees leave the energy sector where do they go?
- How do current employers train their employees to improve their ICS/OT cybersecurity skills?
- How long do ICS/OT cybersecurity employees stay with an employer?
- What are the current pay rates?

Efforts 2: Check Data Categories You Will Collect

- ❑ Raw data and summary analysis of job descriptions of energy sector ICS/OT cybersecurity employment positions that are filled and open.
- ❑ Raw data and summary analysis of how long ICS/OT cybersecurity employees stay with their current employer grouped by employer/job role categories.
- ❑ Raw data and summary analysis of energy sector ICS/OT cybersecurity salaries currently offered by organizational chart categories such as entry-level, mid-level, senior, and/or by job description/skills.
- ❑ Raw data and summary analysis of required and preferred experience and KSAs for entry-level, mid-level, and senior ICS/OT cybersecurity positions from job descriptions and job announcements.
- ❑ Raw data and summary analysis of on-the-job training provided by current employers and categorization of the training as knowledge-based and/or skills/abilities-based.
- ❑ Summary analysis of most frequently requested KSAs for different energy subsectors (electric, oil, and natural gas) and renewable energy providers (wind, solar, geothermal, etc.) for ICS/OT cybersecurity positions.
- ❑ Raw data and summary analysis of the sequence of employers and jobs held by currently employed ICS/OT employees in the energy sector, information on current and former job roles and job descriptions, and how long they stayed with each of their former employers.

Effort 3: ICS/OT Cybersecurity Workforce and Strategic Plan

Gap analysis and recommendations for CESER's cybersecurity workforce strategic plan.

- Complete a gap analysis that identifies needs in the ICS/OT cybersecurity training and workforce development landscape in the energy sector; and
- Develop recommendations and language for a workforce strategic plan based on market assessment results from Efforts 1 and 2.

Eligibility Criteria

- Applicant qualifies as a domestic entity.
- Applicant must certify it is not owned by, controlled by, or subject to the jurisdiction or direction of the government of a Country of Risk.
- National Labs are not eligible to apply directly to this opportunity BUT can be a subcontractor under another organization.
- Individuals are not eligible to apply.

Review Criteria – How Applications Will Be Assessed

- Technical Expertise and Approach (55%)
- Data Security Plan (10%)
- Budget and Milestones (20%)
- Project Team Composition (15%)



Review Criteria

Technical Expertise and Approach (55% total; breakdown below)

- Are the phases of work reasonable, comprehensive, and presented in a logical order? (5%)
- Will the categories of data collected and the analysis results provide comprehensive and novel insights into: ICS/OT cybersecurity workforce and training opportunities; workforce needs; and/or an understanding of the workforce pipeline? (15%)
- Were the methods of analysis appropriate for the type(s) of data collected? (10%)
- Will the proposed final products meet the objectives described in the Opportunity Announcement? (15%)
- Do the applicant's examples of past performance demonstrate the relevant technical expertise to meet the objectives described in the Opportunity Announcement? (10%)

Review Criteria

Data Security Plan (10%)

Are the applicant's data security practices appropriate for the sensitivity of the data and analyses conducted?

Budget and Milestones (20%)



Performer(s) are expected to complete the work within budget and in a 6-month timeframe, with the option of a one-time 3-month no-cost extension. Has the applicant demonstrated the ability to complete the proposed work within the proposed budget and on time?

Project Team Composition (15%)

Does the project team include all necessary performer roles and relevant work experience?

Key Dates

Applications open	11/12/2024
Objective Strategic Session	Released week of November 18 th
Office hours	December 11, 2024, at 2:00 pm ET
Application Deadline	December 23rd, 2024 at 5 p.m. ET
Review and Selection	Expected end of January/early February 2025
Negotiations	1 month after selections have been made
Selectees Announced	Est. March 2025
Activities Begin	Est. March 2025



Thank you for attending the **State of Industrial Control System Cybersecurity Training Opportunity Informational Webinar/Objective Strategic Session (IW/OSS)**

Scan the QR code to learn more about
this Opportunity.

**This recording, transcript and FAQ
will be uploaded to the TechWerx
website.**

