2023

CHEMICAL SECURITY SUMMIT

August 29-31, 2023

#ChemicalSecurity

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

CHEMICAL SECURITY SUMMIT

August 31, 2023

Unmanned Aerial Systems (UAS) Threats Facing the Chemical Sector

Mary Wiegand

Deputy Chief
UAS Security Branch, CISA Security Programs

John Robert

Director
Global Intelligence & Protection, Dow

#ChemicalSecurity

2023 CHEMICAL SECURITY SUMMIT

MANAGING UAS CYBER-PHYSICAL RISK TO CRITICAL INFRASTRUCTURE

Who is CISA

CISA's mission is to lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

The integration of unmanned aircraft systems (UAS) (or drones) into the national airspace system and within critical infrastructure operations has emerged as a particularly concerning physical and cyber threat.

What is CISA Concerned About?

Careless & Clueless

- Consists of most common incidents
- Intent not required to represent a threat
- Unverifiable UAS operator training and UAS maintenance leading to recklessness
- Violates flight restrictions unintentionally or unknowingly

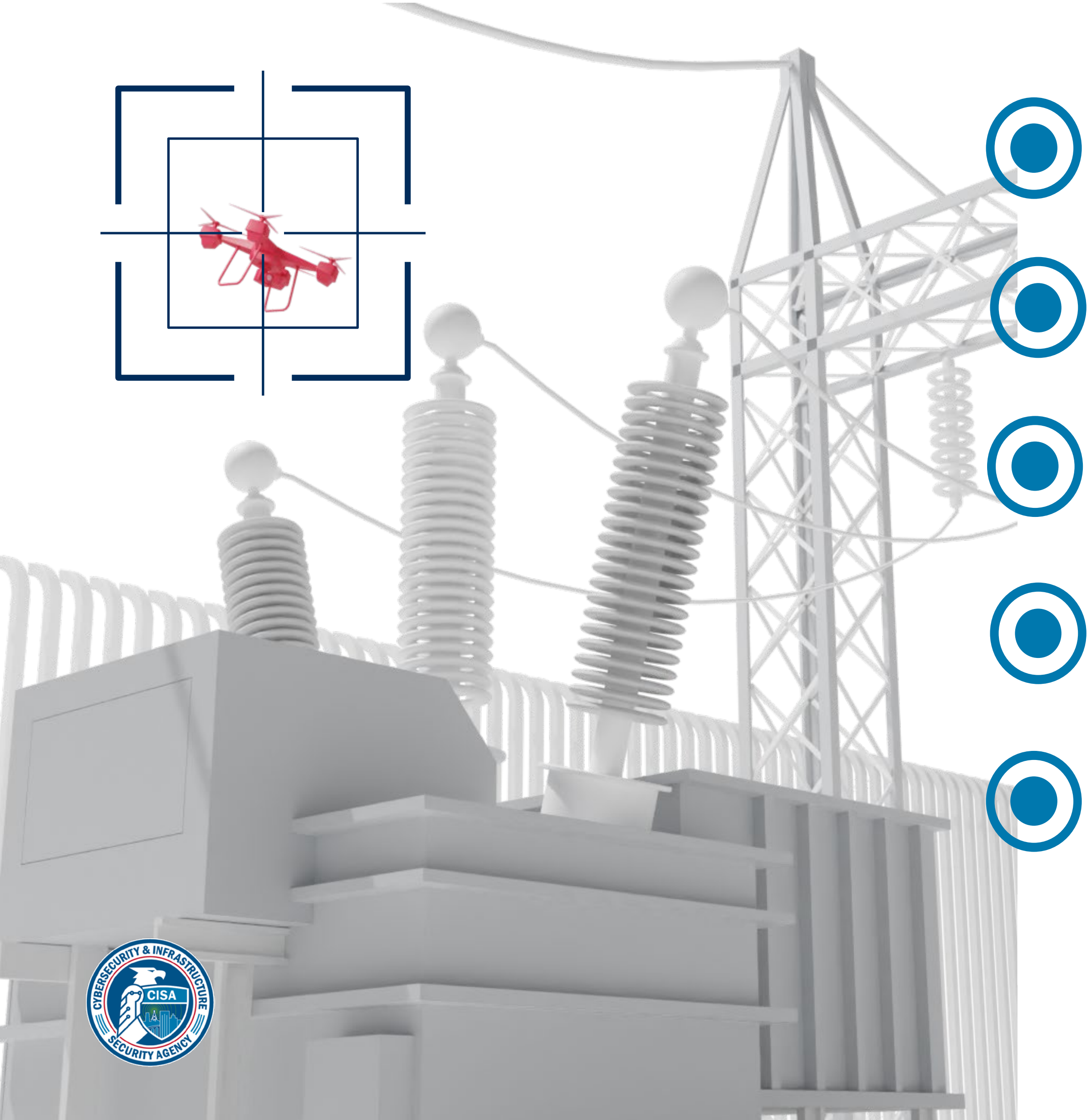
Non-attack nefarious

- Spying to conduct IP theft or espionage
- Pre-operational planning and surveillance
- Disruptions to distract or delay
- Delivery of payloads supporting insider criminal acts

Cyber / physical attack

- Traditional security measures ineffective (gates/guards)
- Close-in blast capable
- Expansive cargo array
    - Payload / drop capable
    - Sprayers
    - Cyber-attack platform
    - Sensors / cameras

Challenges to Mitigating UAS Risk



- Majority of critical infrastructure is owned/operated by the **private sector**
- Airspace above most critical infrastructure is **generally unrestricted**
- Limited/no **air domain awareness** due to legal restrictions/ambiguity when operating detection-only technology
- When detection is possible, **attribution and accountability** are unreliable
- Private sector AND their supporting SLTT law enforcement are **not authorized to use mitigation** technology to counter credible threats

UAS ICTS National Security considerations

Chinese UAS market dominance

Chinese Intelligence Law of 2017

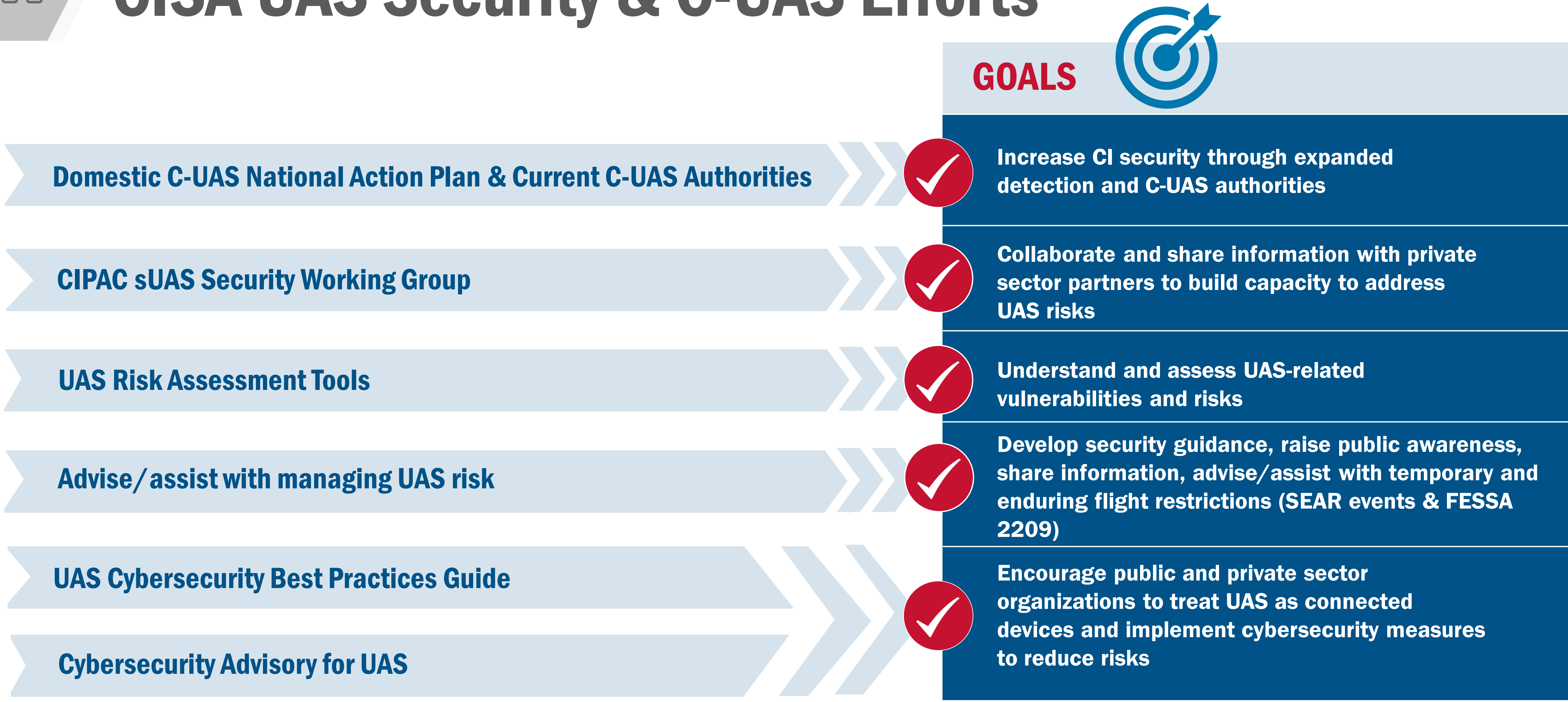
Executive Order 13981

Chinese military-civil designations – 1206h

2023 National Cybersecurity Strategy

2023 ODNI Annual Threat Assessment

CISA UAS Security & C-UAS Efforts



	GOALS
Domestic C-UAS National Action Plan & Current C-UAS Authorities	✓ Increase CI security through expanded detection and C-UAS authorities
CIPAC sUAS Security Working Group	✓ Collaborate and share information with private sector partners to build capacity to address UAS risks
UAS Risk Assessment Tools	✓ Understand and assess UAS-related vulnerabilities and risks
Advise/assist with managing UAS risk	✓ Develop security guidance, raise public awareness, share information, advise/assist with temporary and enduring flight restrictions (SEAR events & FESSA 2209)
UAS Cybersecurity Best Practices Guide	✓ Encourage public and private sector organizations to treat UAS as connected devices and implement cybersecurity measures to reduce risks
Cybersecurity Advisory for UAS	

For more information:

cisa.gov/uas-critical-infrastructure

Questions?

sUAS Security

Email: sUASsecurity@cisa.dhs.gov