READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS
REMS
TECHNICAL ASSISTANCE CENTER
http://rems.ed.gov

Integrating Cybersecurity with Emergency Operations Plans (EOPs) for K-12 Education

Amy Banks, U.S. Department of Education, Center for School Preparedness, Office of Safe and Healthy Students

Hamed Negron-Perez, U.S. Department of Education, Center for School Preparedness, Office of Safe and Healthy Students

Jason Gates, U.S. Department of Homeland Security (DHS), Industry Engagement and Resilience Branch, Office of Cybersecurity and Communications

U.S. Department of Education
Office of Safe and Healthy Students

Welcome & Introductions

Welcome	Housekeeping Items	Speakers

Agenda

Background on the *Guides* and Integrating Cybersecurity into the Six Step Planning Process

Overview of Cybersecurity

Landscape of K-12 Cyber Threats and Trends

DHS Cybersecurity Resources, Programs, and Tools for K-12 Education

Q&A Session

The *Guide*

- Released by the Obama Administration on June 18, 2013
- Developed in collaboration with, and the first joint product of, ED, DHS, FEMA, DOJ, FBI, and HHS
- Accessible at http://rems.ed.gov

Presidential Policy Directive (PPD-8)

National Preparedness Directive

Describes the nation's approach to preparedness

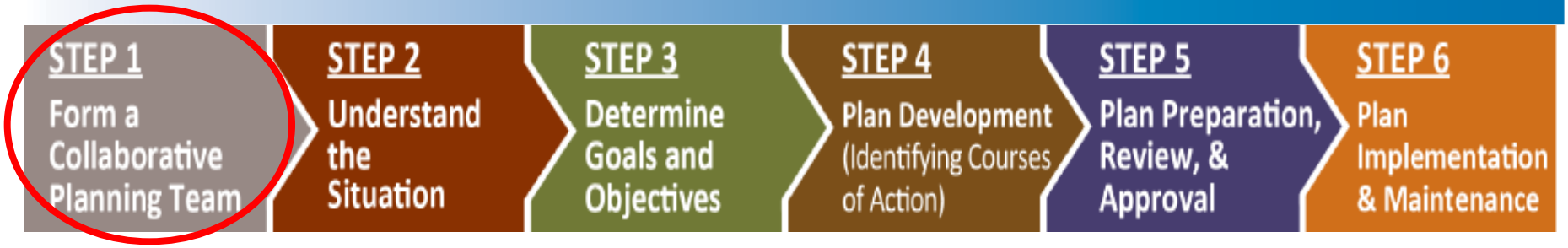
Aims to facilitate an integrated approach and align planning at all levels and with all sectors

Five Preparedness Missions

an incident or emergency

Steps in the Planning Process

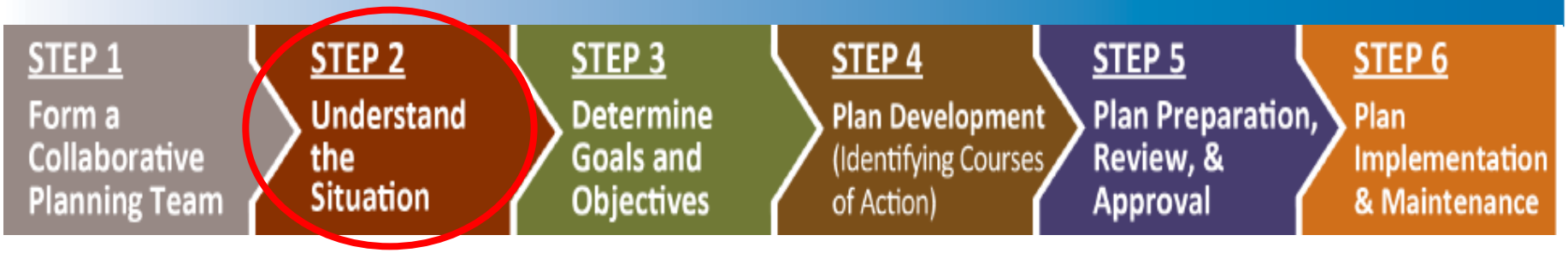
Step 1: Form a Collaborative Planning Team



Team members should include personnel who have a role in both cybersecurity and in managing a cyber incident or emergency. A collaborative planning team may include the representatives from the following areas:

- *Administrators*
- *Educators*
- *Human Resources*
- *Transportation Managers*
- *EMS*
- *Information Technology (IT) and Security Services*
- *Environmental Health and Safety*
- *School Psychologists*
- *Food Personnel*
- *Facilities Managers*
- *U.S. Computer Emergency Readiness Team (US-CERT)*

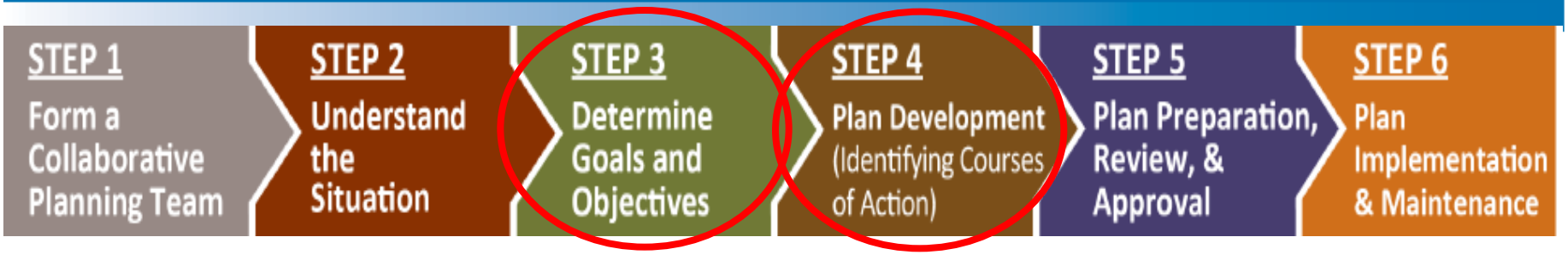
Step 2: Understand the Situation



Step 2

- Identify cyber threats and hazards.
- Assess the cyber risk.
- Identify the cyber vulnerabilities.

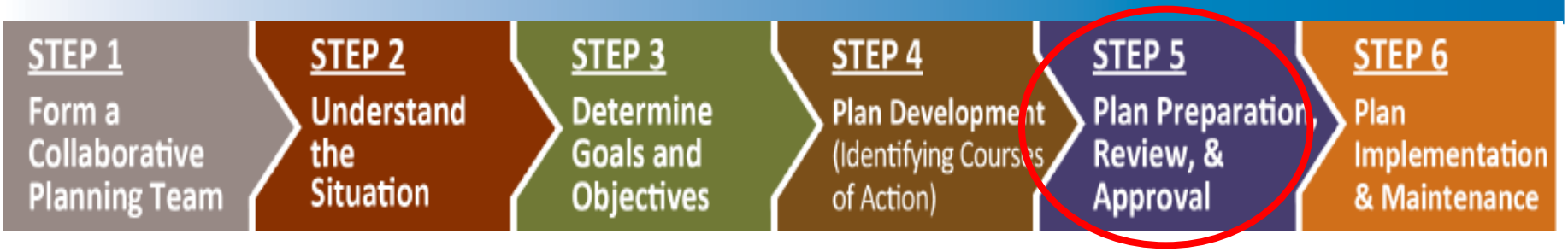
Steps 3 & 4: Develop Goals, Objectives, and Courses of Action



Steps 3 and 4

- Develop goals and objectives for each cyber threat identified in Step 2 and develop a variety of measures to prevent cyber threats.
- Common action steps to address cybersecurity may overlap with other action steps (functions) to address other emergencies.
- These steps may be categorized into a cybersecurity annex or a cyber threat- and hazard-specific annex.

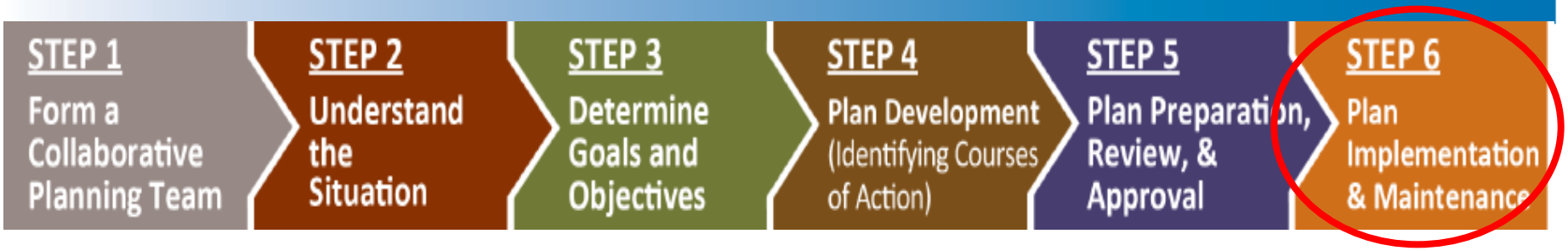
Step 5: Plan Preparation, Review, and Approval



Step 5

- Recommended criteria for a well-designed plan to address cybersecurity include:
  - Addressing how the annex connects to State/county/ municipal plans;
  - Identifying chain of command;
  - Including contact information for key staff; and
  - Clearly identifying roles and responsibilities.

Step 6: Plan Implementation and Maintenance



Step 6

- Train stakeholders on the plan to address cybersecurity.
- Conduct emergency drills and exercises related to cybersecurity.
- Conduct after-action reviews of both drills and actual cyber emergencies.
- Identify lessons learned and implement corrective actions.

Agenda

Background on the *Guides* and Integrating Cybersecurity into the Six Step Planning Process

Overview of Cybersecurity

Landscape of K-12 Cyber Threats and Trends

DHS Cybersecurity Resources, Programs, and Tools for K-12 Education

Q&A Session

Overview

Cyber intrusions, data breaches, and attacks at K-12 schools have increased dramatically over the last decade.

These incidents expose the sensitive personal information of students and staff; disrupt critical operations; and impose high financial costs.

DHS offers a variety of resources, programs, and tools to help K-12 schools establish and maintain secure networks and prevent cyber attacks.

Overview

In coordination with our Federal partners and the private sector, DHS:

- Responds to cyber incidents;
- Provides technical assistance to owners and operators of critical infrastructure; and
- Disseminates notifications regarding current and potential security threats and vulnerabilities.

In addition, the United States Secret Service (USSS) and U.S. Immigration and Customs Enforcement (ICE) investigate Federal cyber crimes, including data breaches, cyber intrusions, and attacks.

Cybersecurity

Cybersecurity is the…

- Prevention of damage to,
- Prevention of unauthorized use of,
- Prevention of exploitation of, and
- Restoration of

… electronic information and communications systems and the information contained therein.

Cybersecurity is a shared responsibility.

Cyber Systems

Business Systems – Mission essential systems that are used to manage or support common business processes and operations.

Control Systems – Cyber systems used to monitor and control sensitive processes and physical functions.

Safety, Security, Support, and Other Specialty Systems – Cyber systems used to manage physical access or for alerting and notification purposes.

Cyber Infrastructure

IT systems support business systems, control systems, and security/safety systems.

Physical security systems may be connected to the Internet, which can introduce cyber vulnerabilities.

Independently addressing the protection of physical and cyber assets is problematic given the interconnected and interdependent nature of the Nation's critical infrastructure.

Cyber Infrastructure

Agenda

Background on the *Guides* and Integrating Cybersecurity into the Six Step Planning Process

Overview of Cybersecurity

Landscape of K-12 Cyber Threats and Trends

DHS Cybersecurity Resources, Programs, and Tools for K-12 Education

Q&A Session

K-12 Cybersecurity In The News

Howard schools recover from possible cyber attack
Baltimore Sun – January 24, 2014
http://www.baltimoresun.com/news/maryland/howard/ellicott-city/ph-ho-cf-hcpss-internet-0123-20140121-story.html

Virginia schools using data system to guide decisions
StateScoop – August 6, 2014
http://statescoop.com/virginia-schools-using-data-system-guide-decisions/

California passes landmark bill to protect students' personal data
Naked Security – September 17, 2014
http://nakedsecurity.sophos.com/2014/09/17/california-passes-landmark-bill-to-protect-students-personal-data/

Personal information of almost 100,000 people exposed through flaw on site for transcripts
Washington Post – October 21, 2014
http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/21/personal-information-of-almost-100000-people-exposed-through-flaw-on-site-for-transcripts/

K-12 Cyber Trends

Trend	Description	Example
Network and Data Breaches	Outside actors gain unauthorized access to computer networks to destroy/disable systems and/or steal data.	In November 2014, a compromised access point within a Kentucky school district's information system resulted in the exposure of several thousand former students' social security data.
Insider Threat	Employees or trusted third parties who intentionally or unintentionally damage/destroy a system and/or steal data.	In July 2014, an employee for a Kansas City school district mistakenly compromised the personal information of nearly 10,000 former and current students after downloading confidential records to a removable hard drive.

Agenda

Background on the *Guides* and Integrating Cybersecurity into the Six Step Planning Process

Overview of Cybersecurity

Landscape of K-12 Cyber Threats and Trends

DHS Cybersecurity Resources, Programs, and Tools for K-12 Education

Q&A Session

Cybersecurity-Specific Documents

Presidential Policy Directive (PPD)-21: Critical Infrastructure Security and Resilience

National Infrastructure Protection Plan (NIPP)

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework**
- **Critical Infrastructure Cyber Community (C^3) Voluntary Program**

DHS Critical Infrastructure Cyber Community Voluntary Program

Critical Infrastructure Cyber Community, or C^3 (pronounced "C Cubed"), Voluntary Program

- An innovative public-private partnership to help connect business, Federal government agencies, academia, and State, local, tribal, and territorial (SLTT) government partners to DHS and other Federal government programs and resources that will assist their efforts in managing their cyber risks and using the NIST Cybersecurity Framework.
- For more information on the C^3 Voluntary Program, visit http://www.dhs.gov/ccubedvp or http://www.us-cert.gov/ccubedvp.
- For a list of cybersecurity and cyber risk management resources for the academic community, visit http://www.us-cert.gov/ccubedvp/getting-started-academia. Each of the resources is cross walked to Core Functions of the NIST Cybersecurity Framework.

DHS Cybersecurity Assessments, Evaluations and Reviews

Cyber Resilience Review (CRR)

- A no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices.
- The CRR may be conducted as a downloadable self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals.
- The review assesses enterprise programs and practices across a range of ten domains, including risk management, incident management, service continuity, and others.
- For more information, visit http://www.us-cert.gov/ccubedvp/self-service-crr.

Cybersecurity Evaluation Tool (CSET)

- A self-assessment tool that provides prioritized recommendations and enables users to assess their network and industrial control system security practices against industry and government standards.
- Organizations can also request **On-Site Cybersecurity Consulting,** a facilitated site visit that could include basic security assessments, network architectural review and verification, network scanning using custom tools to identify malicious activity and indicators of compromise, and penetration testing.
- For more information, visit http://ics-cert.us-cert.gov/assessments.

DHS Cybersecurity Assessments, Evaluations and Reviews, Continued

Cybersecurity Advisors (CSAs)

- Regionally located DHS personnel who direct coordination, outreach, and regional support to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's critical infrastructure and SLTT governments.
- CSAs offer immediate and sustained assistance to prepare and protect SLTT governments and private entities.
- For more information, email cyberadvisor@hq.dhs.gov.

Protective Security Advisors (PSAs)

- Trained critical infrastructure protection and vulnerability mitigation subject matter experts.
- The PSA program focuses on physical site security and resiliency assessments, planning and engagement, incident management assistance, and vulnerability and consequence information sharing.
- For more information, visit http://dhs.gov/protective-security-advisors.

DHS Cybersecurity Information Sharing and Collaboration

Cyber Information Sharing and Collaboration Program (CISCP)

- Enhances cybersecurity collaboration between DHS and critical infrastructure owners and operators, and leverages government and industry subject matter expertise to collaboratively respond to cybersecurity incidents.
- For more information about CISCP, please email ciscp_coordination@hq.dhs.gov.

DHS's Enhanced Cybersecurity Services (ECS) program

- Supports voluntary information-sharing to assist and improve the protection of critical infrastructure systems from unauthorized access, exploitation, or data exfiltration. The program shares cyber threat information with qualified commercial service providers.
- For more information about ECS, please visit http://www.dhs.gov/enhanced-cybersecurity-services, or email ECS_Program@HQ.DHS.gov.

DHS Cybersecurity Alerts and Incident Response Assistance

National Cybersecurity & Communications Integration Center (NCCIC)

- A central location where a diverse set of public- and private-sector partners involved in cybersecurity and communications protection coordinate and synchronize their efforts.
- Analyzes cybersecurity and communications information, shares timely and actionable information, and coordinates response mitigation and recovery efforts.
- For more information, visit https://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

United States Computer Emergency Readiness Team (US-CERT)

- Collaborates with government, private sector, research community, and international entities to monitor cyber trends.
- Provides access to actionable situational awareness reports; detection information about emerging cyber threats and vulnerabilities, and cybersecurity warning and alert notifications through the **National Cyber Alert System**.
- For more information, visit http://www.us-cert.gov/.

DHS Cybersecurity Awareness Campaigns

National Cybersecurity Awareness Month (NCSAM)

- Occurs each October and is designed to engage and educate the public and private sectors to create a safe, secure, and resilient cyber environment.
- Raises awareness about cybersecurity through a series of events and programs across the country.
- For more information, visit http://www.dhs.gov/national-cyber-security-awareness-month.

Stop.Think.Connect.™ campaign

- A national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online.
- Offers resources and tips for students, young professionals, and educators.
- For more information, visit http://www.dhs.gov/stopthinkconnect.

DHS Law Enforcement Resources

United States Secret Service (USSS) and Immigration and Customs Enforcement (ICE)

- DHS law enforcement agencies with jurisdiction over a wide range of Federal crimes that include, but are not limited to, cybercrime, financial crime, and identity theft.
- To report information about possible cyber crime activity, contact your local **USSS** or **ICE** field offices. For more information, visit www.secretservice.gov or www.ice.gov.
- USSS operates the **Electronic Crimes Task Forces (ECTF)**
  - A network of regional task forces that partner to prevent, detect, mitigate, and investigate various cyber crimes. ECTFs bring together not only Federal, State and local law enforcement, but also prosecutors, private industry, and academia.
  - More than 200 academic institutions are ECTF members.
  - For more information, visit www.secretservice.gov/ectf.shtml.

Additional DHS Resources

Additional tools and resources are also available for school officials to use as part of their analytical and protective measures efforts. These include, but are not limited to:

- National Initiative for Cybersecurity Education (NICE) resources;
- National Initiative for Cybersecurity Careers and Studies (NICCS) Portal;
- Cybersecurity Workforce Planning Diagnostic;
- National Cybersecurity Workforce Framework;
- National Centers of Academic Excellence (CAE) resources; and

For more information related to these resources, as well as resources supporting cybersecurity career development and workforce planning, please visit www.us-cert.gov/ccubedvp.

Related Resources & Support

Multi-State Information Sharing and Analysis Center (MS-ISAC)

- The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's SLTT governments. The MS-ISAC 24x7 cybersecurity operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response.
- For more information, email: info@msisac.org

Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)

- The REN-ISAC aids and promotes cybersecurity operational protection and response within the higher education and research (R&E) communities; within the context of a private community of trusted representatives at member institutions; and in service to the R&E community at-large.
- For more information, visit http://www.ren-isac.net/

Related Resources & Support

If you want to receive alerts about **current security issues or vulnerabilities**, visit http://www.us-cert.gov/ncas/alerts/.

If you are interested in **conducting a cybersecurity assessment**, visit http://www.us-cert.gov/ccubedvp/self-service-crr.

If you are interested in **increasing cyber awareness among your students and staff**, visit http://www.dhs.gov/stopthinkconnect.

Integrating Cybersecurity into your School EOP

The Six Step Planning Process

- Form a Collaborative Planning Team
- Understand the Situation
- Determine Goals & Objectives
- Plan Development
- Plan Preparation, Review, & Approval
- Plan Implementation & Maintenance

Agenda

- Background on the Guides & Integrating Cybersecurity into the Six Step Planning Process
- Overview of Cybersecurity
- Landscape of K-12 Cyber Threats and Trends
- DHS Cybersecurity Resources, Programs, and Tools for K-12 Education
- **Q&A Session**

Questions?

Remember to pose your question using the Q&A Chat function on the lower right side of your computer screen.

The REMS TA Center

READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS
REMS
TECHNICAL ASSISTANCE CENTER

Phone: (855) 781-7367 (REMS)
Email: info@remstacenter.org

http://rems.ed.gov

Get the *Guide*

Join our Community of Practice

Access Virtual Trainings

Request an On-site Training