NICE Conference and Expo 2019

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

WHAT IS YOUR RECIPE FOR SMALL BUSINESS CYBERSECURITY RESILIENT ECOSYSTEMS?

PARTNERING FOR A STRONGER CYBERSECURITY COMMUNITY

CASCADE
California Advanced Supply Chain Analysis & Diversification Effort

Eileen Sanchez
State of California

Today At-A-Glance

- Why you? Why Cyber? Why Collaborate?
- Overview of cybersecurity resilience ingredients and examples
- Group breakouts
- Interactive discussion

CASCADE
California Advanced Supply Chain Analysis & Diversification Effort

NICE Conference and Expo 2019
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Workshop Takeaways

- Identify various stakeholders involved in building small business cybersecurity resilient ecosystem
- Learn about others' contacts and stakeholders involved
- Gain a better understanding of how to build collaboration and coalitions between regions

CASCADE
California Advanced Supply Chain Analysis & Diversification Effort

NICE Conference and Expo 2019
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Why you? Why Cyber? Why Collaborate?

Three Key Questions

- What is Happening?
- How does it Impact Me?
- How am I a Part of the Solution?

Why Small Business Cybersecurity?

Risk management is a fundamental principle of cybersecurity. Adversaries and threats are constantly changing and evolving.

- There are 30.2 million small businesses in the USA, which comprise a whopping 99.9% of all USA businesses.(Small Business Administration)
- Half of all cyberattacks are aimed at small businesses (and it takes an average of 6 months to detect a breach!) (Small Business Trends)
- Types of evolving threats for small businesses
    - External Attacker
    - Insider Threat
    - Supply Chain Risk

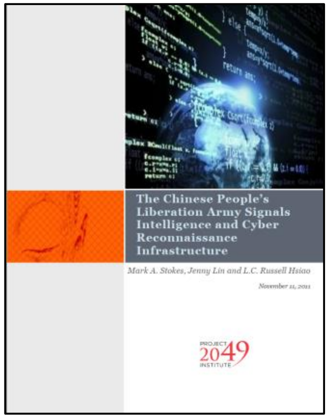
Which is Bigger?

U. S. MARINE CORPS

End of FY 2019 – Authorized End Strength of 186,100 Active Personnel*

End Strength from:
https://www.jcs.mil/Media/News/News-Display/Article/1601323/president-signs-fiscal-2019-defense-authorization-act-at-fort-drum-ceremony/

CHINA’S CYBER WARRIORS



The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure

Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao

November 11, 2011

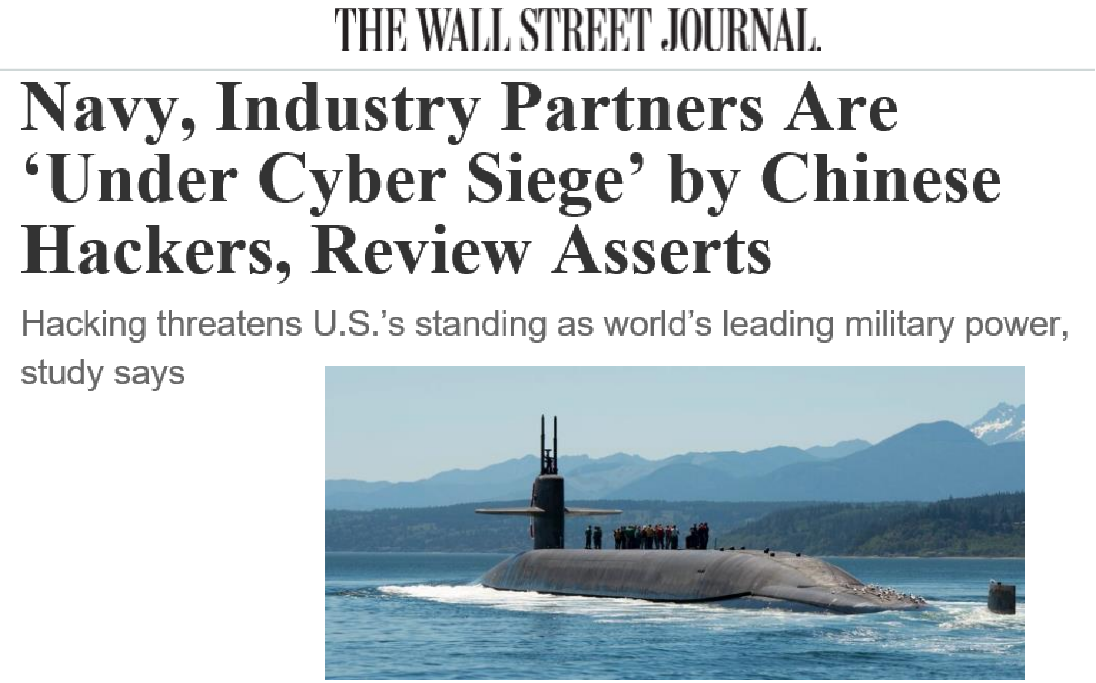
PROJECT 2049 INSTITUTE

“State-sponsored cyber espionage is ubiquitous, with more than 100 countries actively hacking the systems of other countries and businesses. China alone has developed an army of 180,000 cyber spies and warriors.” (Goodman, 2015, p. 31)

Reference: Goodman, M. (2015). ***Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It.*** Doubleday ISBN: 978-0-53900-5.

China could have more Cyber Warriors than Active Duty Marines in the Marines Corp

State of Industry Cybersecurity



THE WALL STREET JOURNAL.

Navy, Industry Partners Are 'Under Cyber Siege' by Chinese Hackers, Review Asserts

Hacking threatens U.S.'s standing as world's leading military power, study says

Photo: Navy Times March 13, 2019

"Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners." (p. 5)

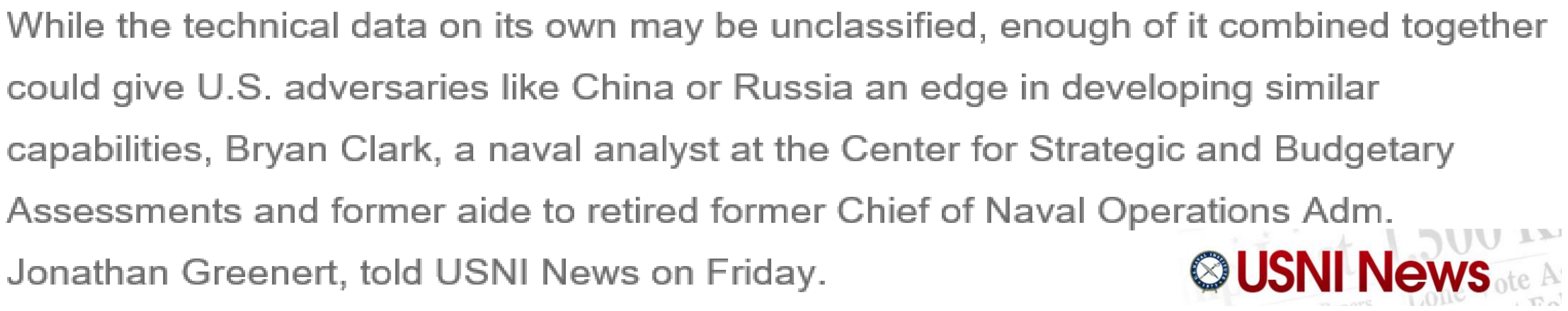
Photo: Navy Times March 13, 2019

STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT

OF THE US INTELLIGENCE COMMUNITY

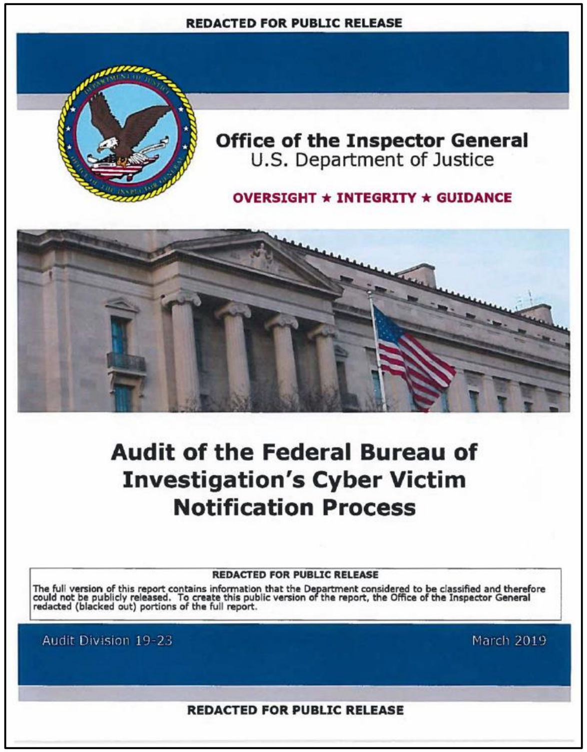
Daniel R. Coats
Director of National Intelligence



While the technical data on its own may be unclassified, enough of it combined together could give U.S. adversaries like China or Russia an edge in developing similar capabilities, Bryan Clark, a naval analyst at the Center for Strategic and Budgetary Assessments and former aide to retired former Chief of Naval Operations Adm. Jonathan Greenert, told USNI News on Friday.

USNI News

$600 billion of IP loss



REDACTED FOR PUBLIC RELEASE

Office of the Inspector General
U.S. Department of Justice

OVERSIGHT ★ INTEGRITY ★ GUIDANCE

Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process

REDACTED FOR PUBLIC RELEASE

The full version of this report contains information that the Department considered to be classified and therefore could not be publicly released. To create this public version of the report, the Office of the Inspector General redacted (blacked out) portions of the full report.

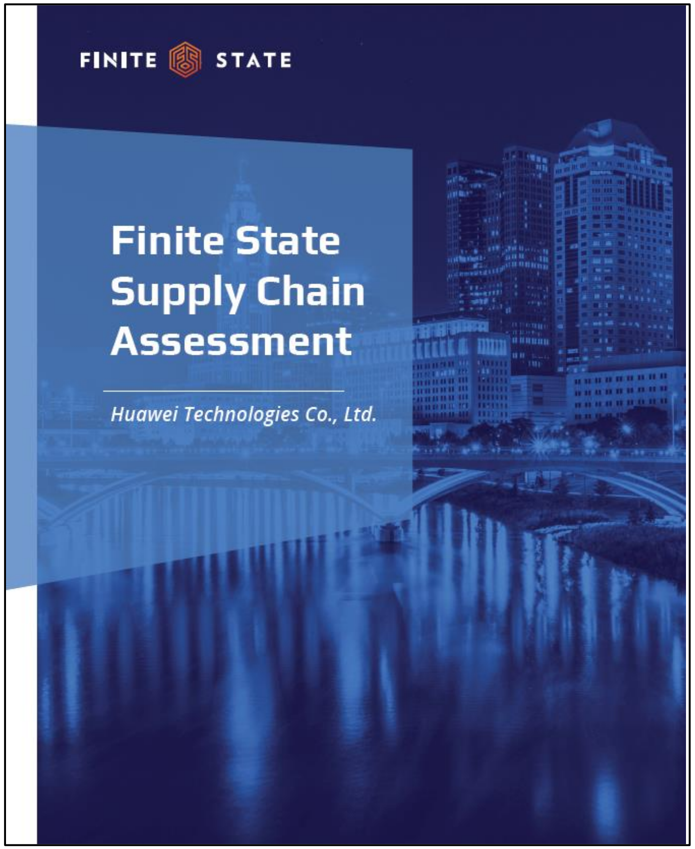
Audit Division 19-23

March 2019

REDACTED FOR PUBLIC RELEASE

In the redacted March 2019 U.S. Department of Justice Office of Inspector General Report, *Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process,* dated March 2019, "the **FBI had 721 Special Agents dedicated to cyber investigations**, including cyber victim notifications" (p. 1). Over the period from November 2014 to December 2017, "Cyber Guardian had **16,409 cyber incidents and 20,803 victim notifications**" (p. 12). Of special note was another revealing comment. "According to FBI personnel, victims of cyber intrusions are typically identified by the FBI or its partner agencies in the course of their investigative activities. As a result, many cyber victims, **most of which are companies or organizations, are unaware that they are victims of an intrusion until the FBI notifies them**." (p. 1)

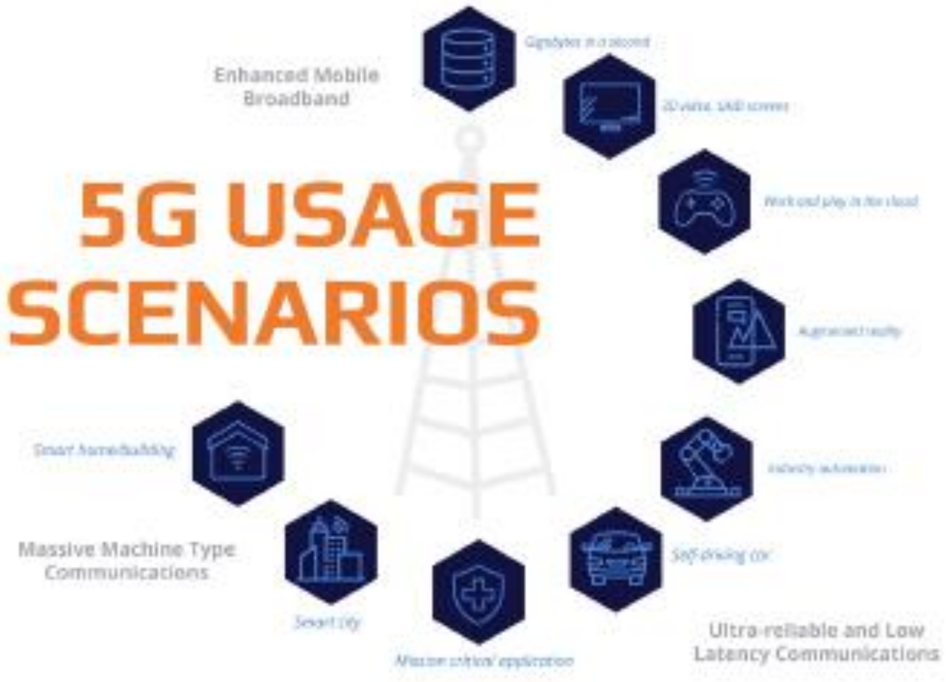
Supply Chain



FINITE STATE

Finite State Supply Chain Assessment

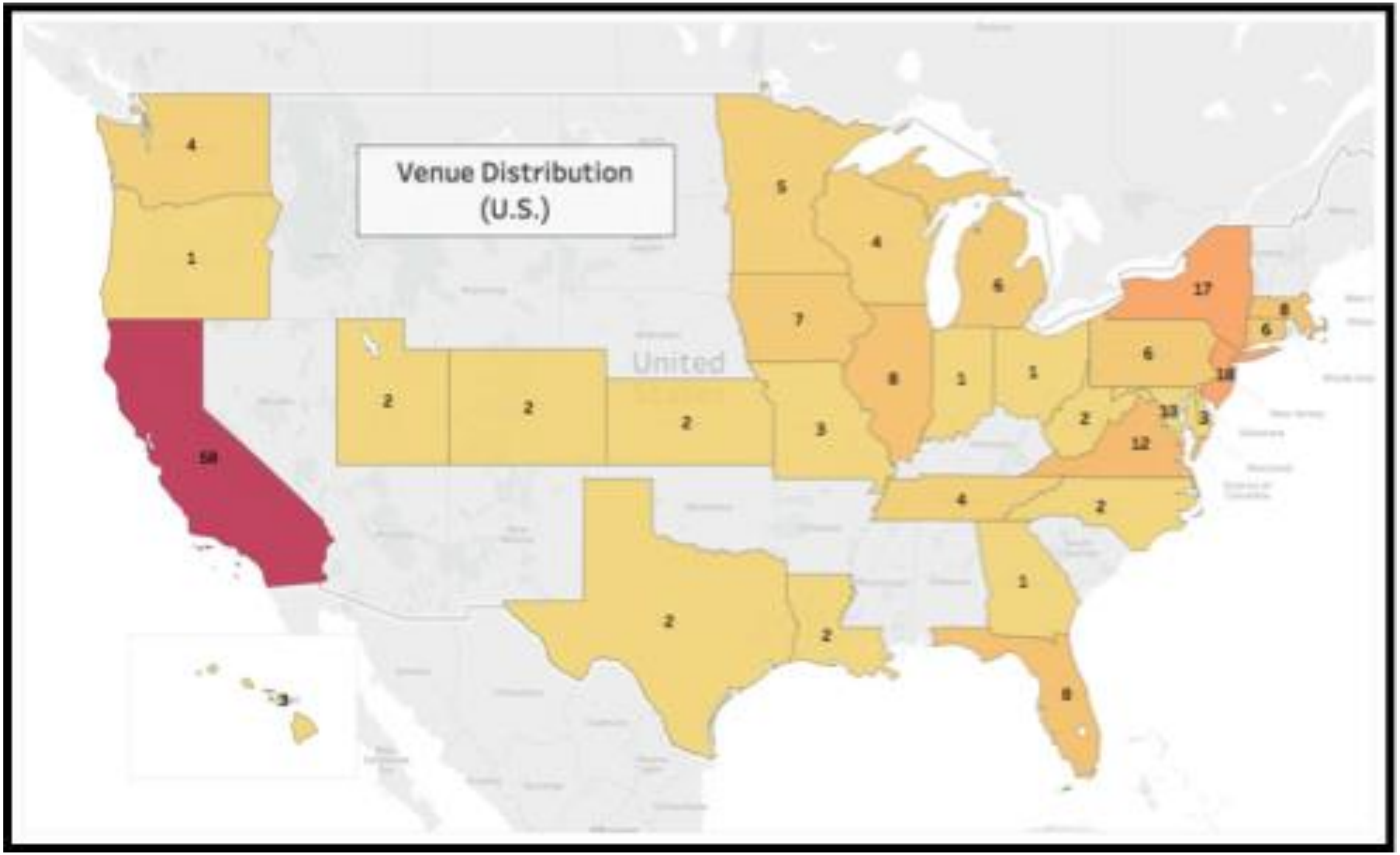
Huawei Technologies Co., Ltd.


5G USAGE SCENARIOS
Enhanced Mobile Broadband
Gigabytes in a second
3D video, UHD screen
Work and play in the cloud
Augmented reality
Industry automation
Self driving car
Ultra-reliable and Low Latency Communications
Mission critical application
Smart city
Massive Machine Type Communications
Smart home/building

"5G networks are ***highly distributed****,* ***complex to secure****, and* ***reliant upon long supply chains*** *dominated by one Original Equipment Manufacturer (OEM), Huawei, and the consequences of* ***even relatively isolated attacks*** *on 5G network components could* ***cause cascading failures leading to loss of critical services****.* ***Given this threat landscape****, it is understandable that 5G has become a focal point for international policy debates."* (p. 8)

Distribution of Chinese Espionage Cases in USA

California Advanced Supply Chain Analysis & Diversification Effort



[A Blueprint To Stop Chinese Espionage, IP Theft: Nick Eftimiades, Top Intel Expert](https://breakingdefense.com/2018/12/how-to-combat-chinese-espionage-ip-theft-nick-eftimiades-top-intel-expert/)

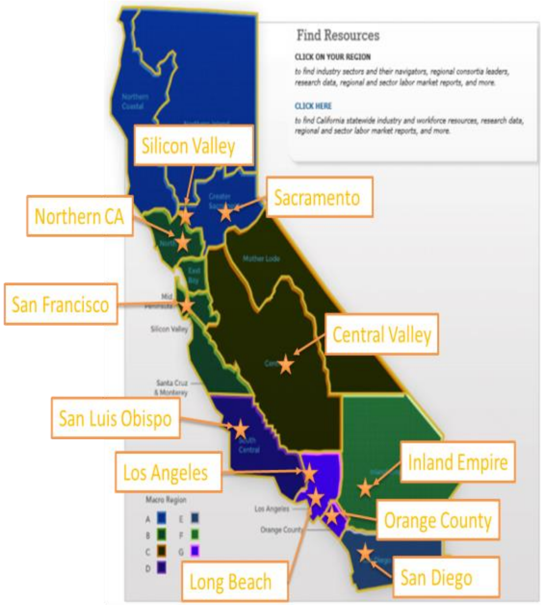
https://breakingdefense.com/2018/12/how-to-combat-chinese-espionage-ip-theft-nick-eftimiades-top-intel-expert/

Grassroots Approach

CASCADE
California Advanced Supply Chain Analysis & Diversification Effort

Regional Community Impact & National Collaboration

TEAM USA



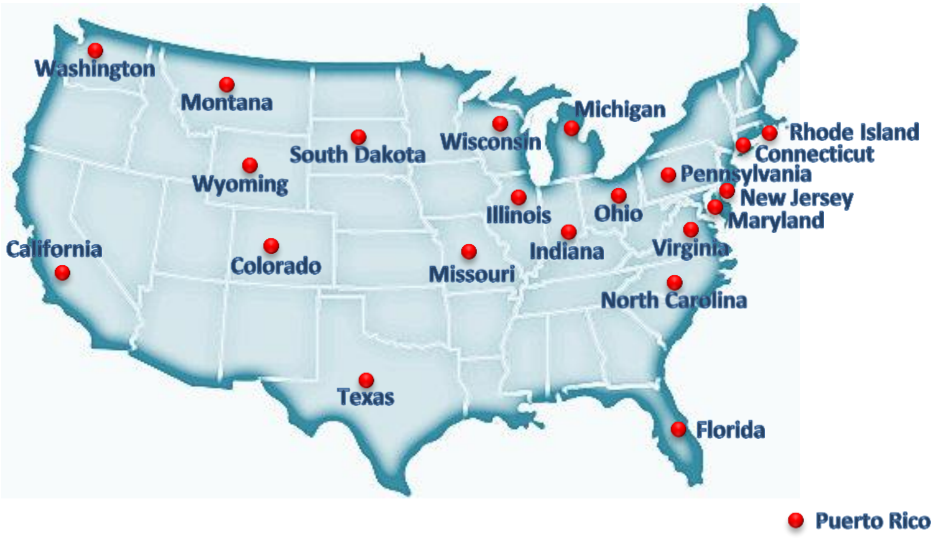
Find Resources

CLICK ON YOUR REGION

to find industry sectors and their navigators, regional consortia leaders, research data, regional and sector labor market reports, and more.

CLICK HERE

to find California statewide industry and workforce resources, research data, regional and sector labor market reports, and more.



Cyber Defenses Must Change

- ✓ Supply chain
- ✓ Don’t know
- ✓ Doesn’t impact me
- ✓ Too expensive
- ✓ Just another Gov’t Regulation

“ We should not wait until an adversary is in our networks or on our systems to act“

Command Vision for US Cyber Command

Why you? Why Cyber? Why Collaborate?

CASCADE
California Advanced Supply Chain Analysis & Diversification Effort

- **The Cyber Threat is Real & Significant**
  - Security by Obscurity is over in the Current & Future Threat Environment
  - Inaction is no longer an option
  - Impacts (economical, social, & lifestyle) could be Severe
- **Our Shared Future**
  - You can be a Critical Partner in this Effort
  - WE can make a difference
  - Implementation will occur on multiple fronts

NICE Conference and Expo 2019

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Cybersecurity Resilience Ingredients

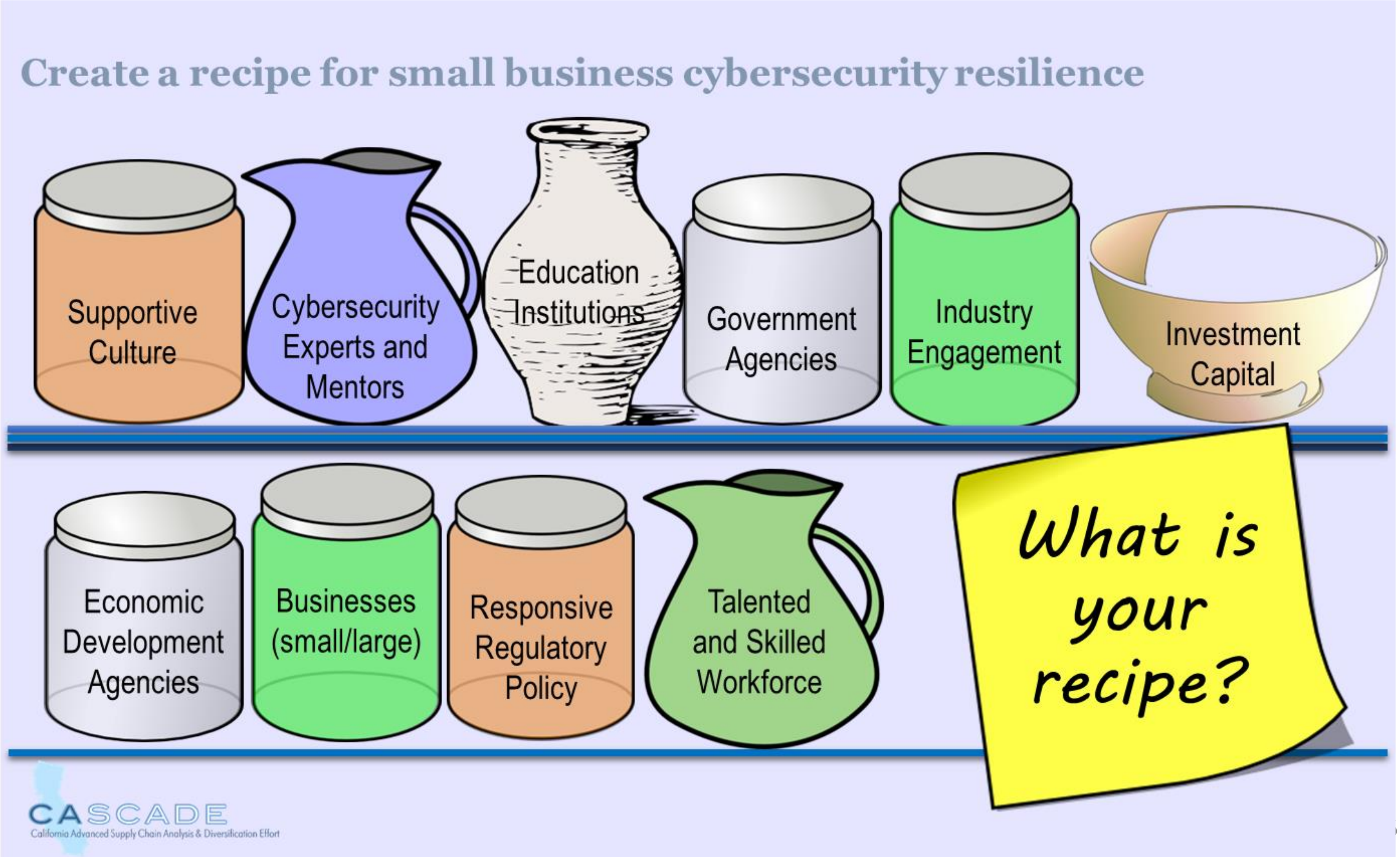
CASCADE

California Advanced Supply Chain Analysis & Diversification Effort

WHAT IS YOUR RECIPE FOR
SMALL BUSINESS CYBERSECURITY
RESILIENT ECOSYSTEMS?

PARTNERING FOR A STRONGER CYBERSECURITY COMMUNITY

Cybersecurity Resiliency Recipe



Create a recipe for small business cybersecurity resilience

Supportive Culture
Cybersecurity Experts and Mentors
Education Institutions
Government Agencies
Industry Engagement
Investment Capital
Economic Development Agencies
Businesses (small/large)
Responsive Regulatory Policy
Talented and Skilled Workforce
CASCADE
California Advanced Supply Chain Analysis & Diversification Effort

What is your recipe?

NICE Conference and Expo 2019
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Group Breakouts

1. Identify your community – local, regional, statewide, national?
2. What ingredients do you have now?
3. What ingredients do you need?
4. Where can you find the missing ingredients?
5. Do others in your group have similar/different recipes?

CASCADE
California Advanced Supply Chain Analysis & Diversification Effort

WHAT IS YOUR RECIPE FOR
SMALL BUSINESS CYBERSECURITY
RESILIENT ECOSYSTEMS?
PARTNERING FOR A STRONGER CYBERSECURITY COMMUNITY

NICE Conference and Expo 2019
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Interactive Discussion

CASCADE
California Advanced Supply Chain Analysis & Diversification Effort

WHAT IS YOUR RECIPE FOR
SMALL BUSINESS CYBERSECURITY
RESILIENT ECOSYSTEMS?

PARTNERING FOR A STRONGER CYBERSECURITY COMMUNITY