



ENABLING COLLECTIVE CYBER DEFENSE

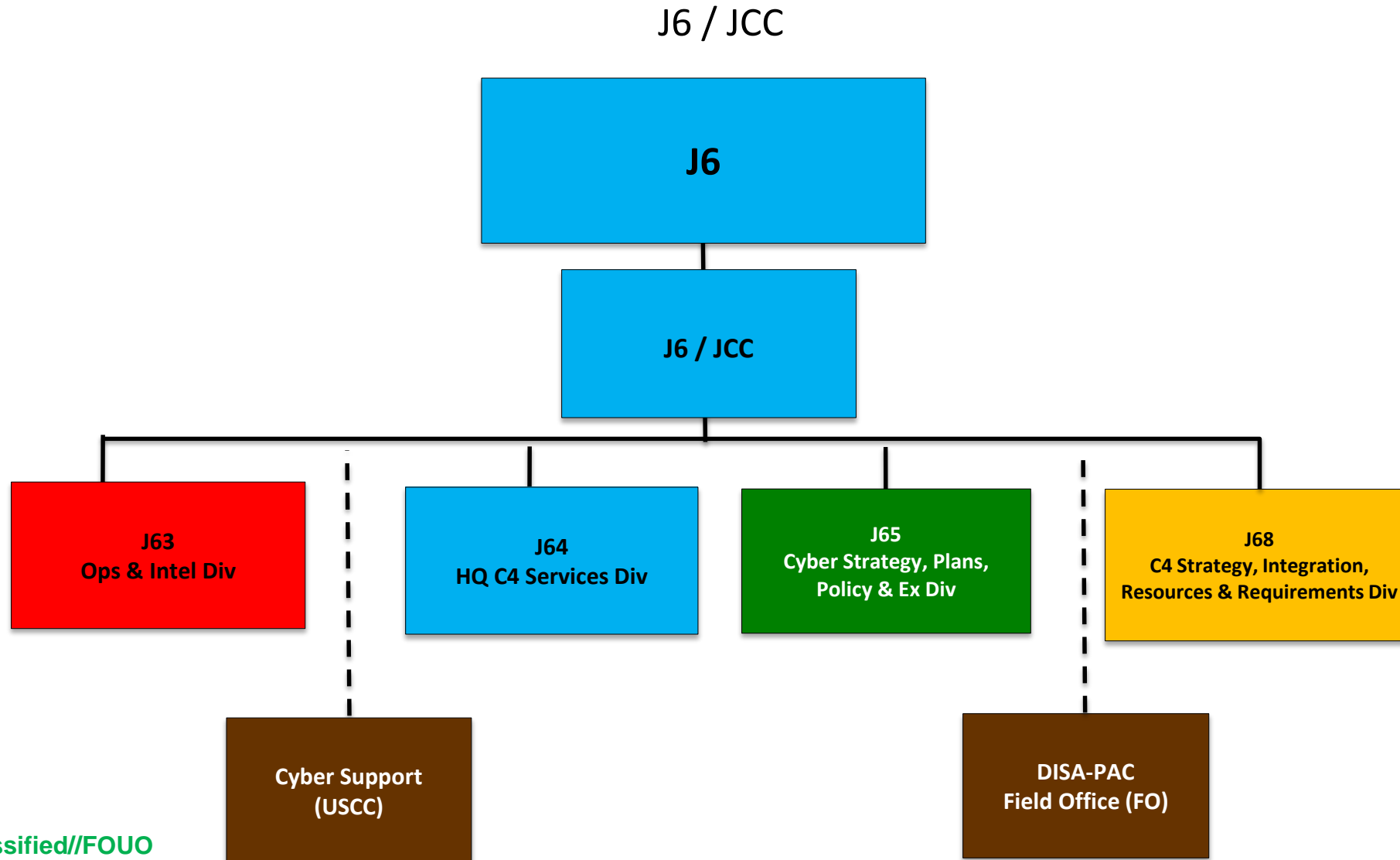
DEFENDING THE DODIN/DII

This briefing is:

UNCLASSIFIED//FOR OFFICIAL USE ONLY



PACOM

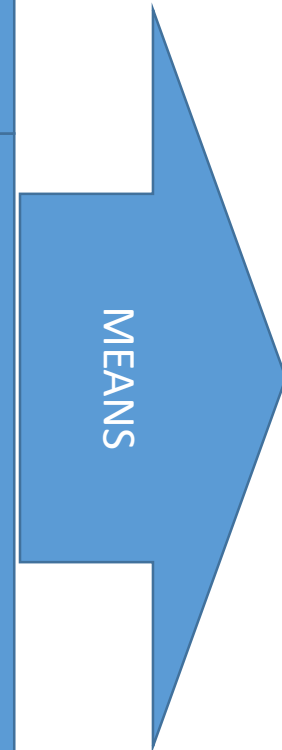




JAPAN and U.S. CYBER EFFORTS

- Guidelines for JPN-U.S. Cooperation in Cyberspace

PURPOSE	Take appropriate actions to respond to events that threatens the Confidentiality, Availability and Integrity of our shared information resources and systems
WAYS	<p>Information sharing on threats and vulnerabilities.</p> <p>Information sharing on the development of various capabilities in cyberspace including best practices on training, education and workforce development.</p> <p>Information sharing to help protect critical infrastructure and services.</p> <p>Maintain a posture to monitor respective shared networks and systems.</p> <p>Ensure resiliency of our respective networks and systems.</p> <p>Contribute to the whole of government efforts to improve cybersecurity.</p> <p>Participate in bilateral exercises.</p>



CDPWG
Cyber Defense Policy Working Group
Cyber Dialogue

CONTENTS
Governance, authority, policy, regulation, legal etc.

IAWG
Information Assurance Working Group

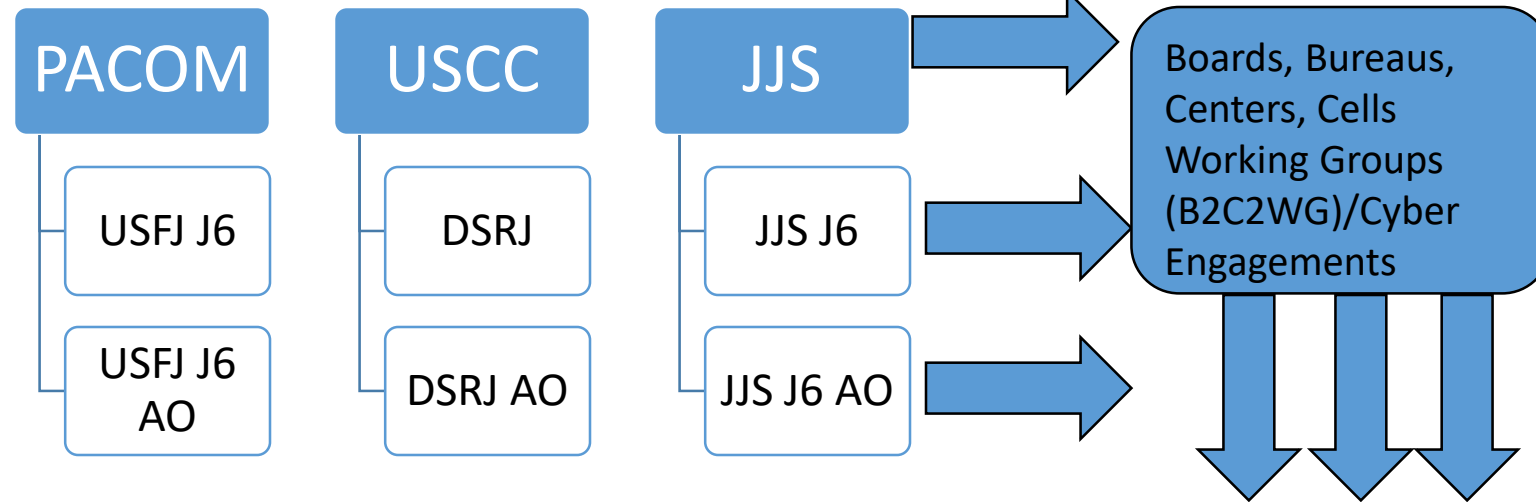
CONTENTS
Concrete measures aimed at deepening information sharing, systems/capabilities and workforce development

Evaluate IAWG measures through bilateral exercises (Keen Edge, Keen Sword, Defensive Cyber Symposium etc.)

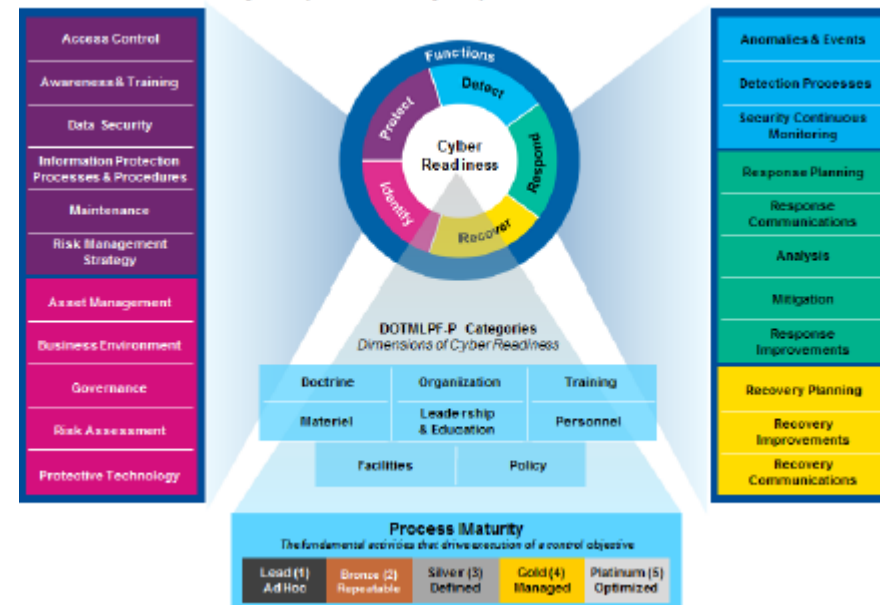




BILATERAL CYBER ROAD MAP



Cyberspace Security Capabilities Framework





MIL TO MIL Engagements

- **Working Groups**

- Information Assurance (IAWG) – Biannual
- Cyber Defense Policy (CDPWG) – Biannual
- Monthly Talks – Monthly – Japan

- **Symposiums**

- Sr Communicators Symposium (SCS) – Biannual
- Defensive Cyber Symposium – On-Going
- Capture the Flag Event – Annual

- **Exercises**

- Pacific Sentry (PACOM) – Annual
- Keen Edge (USFJ) – 2 yr
- Keen Sword (USFJ) – 2 yr
- Yama Sakura (Components) – Annual
- Resilient Shield (Components) – Annual
- Orient Shield (Components) – Annual
- Ulchi-Focus Guardian (Components) – Annual



Bilateral Cyber Solution

How do you know what or how much security you need?

Assessment survey helps to identify security requirements and knowledge gaps based on operational needs, threats, and impact from those threats

Cyberspace Capabilities Survey

Capabilities Identification and prioritization

Identify and prioritize capabilities and gaps based on operational needs, threats, and impact from those threats critical to moderate

Four concrete steps to improving bilateral cyber resiliency for systems, platforms and personnel

Reassessment Capability Survey

Action Plan

Apply corrective measures such as adding tools, techniques and procedures, tightening policies, training for personnel and workforce development

Test to check that corrective measures implemented are effective and identify any new security flaws or capability gaps



TAKE AWAYS

- **Significant Cybersecurity Focus**
- **Many Cyber Engagements in Various Maturity Stages**
- **Enhance Cyber Bilateral Operations**



QUESTIONS?