RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AST1-R05

CForum: A Community Approach for Improving Cybersecurity Programs

Tom Conkle
Cybersecurity Engineer
G2, Inc.
@TomConkle

Greg Witte
Sr. Cybersecurity Engineer
G2, Inc.
@TheNetworkGuy

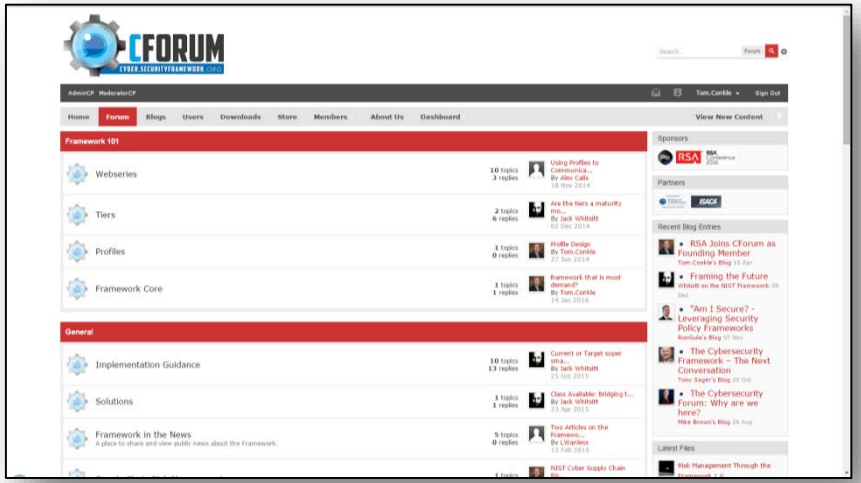
CForum is an online community working together to improve cybersecurity

- CForum continues the conversation started during the NIST Cybersecurity Framework workshops as:
  - a place to collaborate about measuring and improving cybersecurity
  - an environment for discussing emerging threats to cybersecurity information and operation technology
  - a forum for thought leaders to share information

Cyber.SecurityFramework.org

We will answer several primary questions regarding CForum today

- Why was CForum established?
- What are the objectives of CForum?
- How do you use CForum?



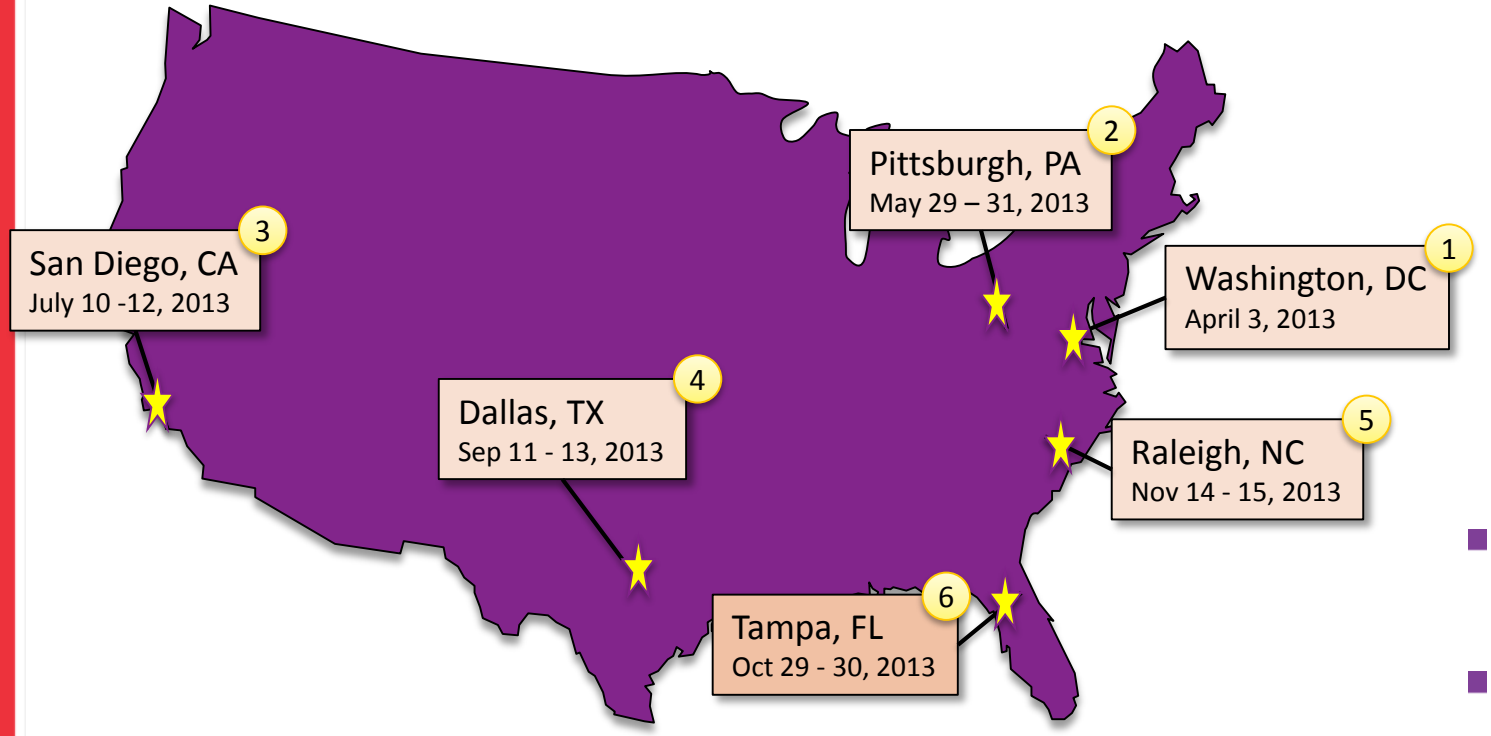
Format of the presentation follows the CSF steps

CSF Steps 1 and 2
Prioritize, Determine Scope and Orient

Executive Order 13636 asked for the creation of a Cybersecurity Framework for all sectors

- Executive Order Requirements
  - Be flexible
  - Be non-prescriptive
  - Leverage existing approaches, standards, practices
  - Be globally applicable
  - Focus on risk management vs. rote compliance
- Framework for Improving Critical Infrastructure Cybersecurity
  - Referred to as “The Framework”
  - Issued by NIST on February 12, 2014.

CForum continues the dialogue started during the Framework Development



- NIST Conducted 5 workshops
- Released 3 RFIs

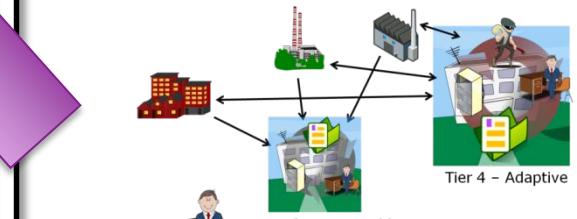
The Framework establishes three primary components

ILLUSTRATIVE

Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	COBIT 5 APO13.01 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1 controls
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	COBIT 5 APO13.12 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	COBIT 5 MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1
PROTECT (PR)	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	CCS CSC 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	ISA 62443-3-3:2013 SR 6.1 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	COBIT 5 BAI01.10 CCS CSC 18 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	COBIT 5 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	CCS CSC 8 COBIT 5 DSS01.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	COBIT 5 BAI07.08 ISA 62443-2-1:4.4.3.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	COBIT 5 EDM03.02
		RC.CO-2: Reputation after an event is repaired	COBIT 5 MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	NIST SP 800-53 Rev. 4 CP-2, IR-4

Implementation Tiers



Framework Profiles

Function	Category	Subcategory	Priority	Org Policy	Org Practices	Status	Comments / Evidence
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	M				
		ID.AM-2: Software platforms and applications within the organization are inventoried	L				
		ID.AM-3: Organizational communication and data flows are mapped	H				
		ID.AM-4: External information systems are catalogued	M				
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on	M				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire [illegible] and third-[illegible]	H				

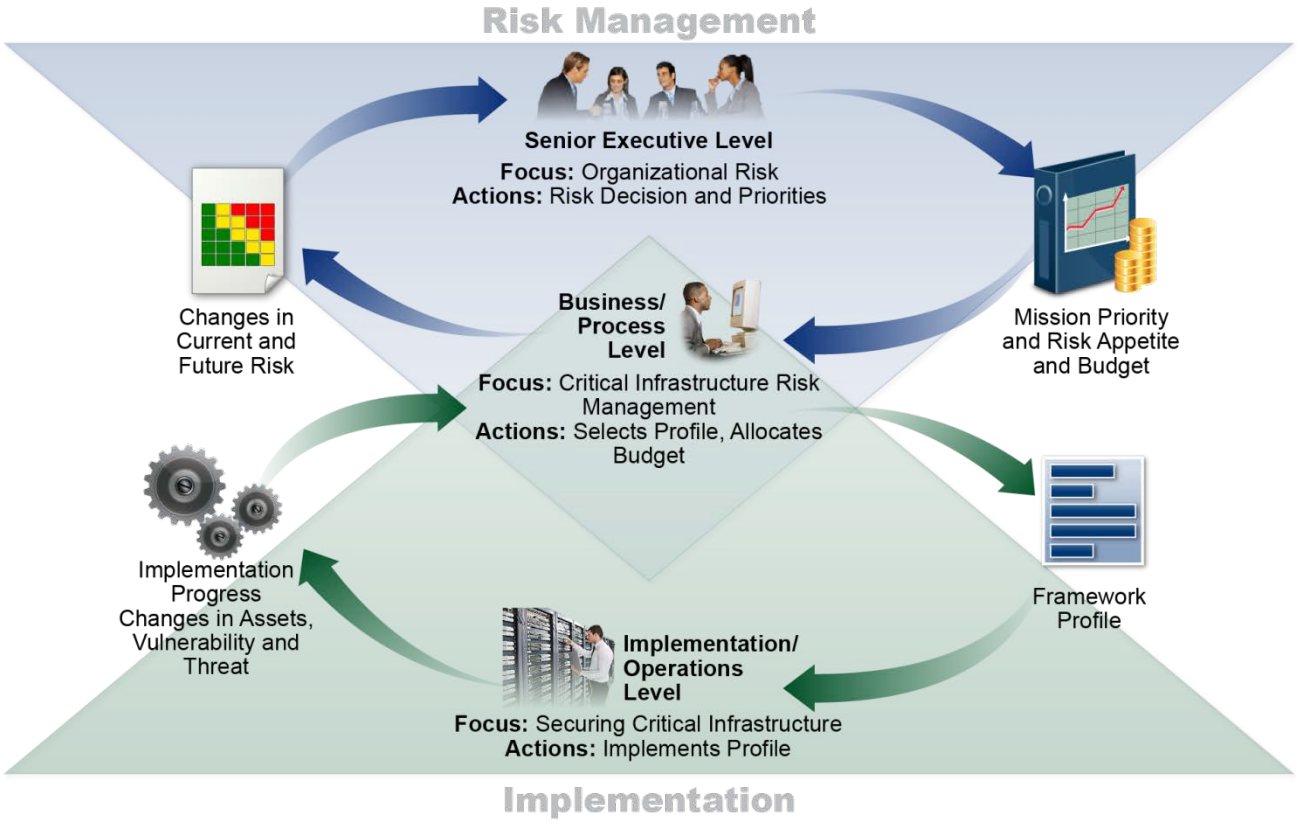
The Framework Core establishes a common language

- Consists of 5 Functions
  - Identify, Protect, Detect, Respond, Recover
- Describes a set of cybersecurity activities, desired outcomes
- Includes references to industry proven standards
- Three levels (Function, Categories, and Subcategories) of fidelity

Framework Core

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

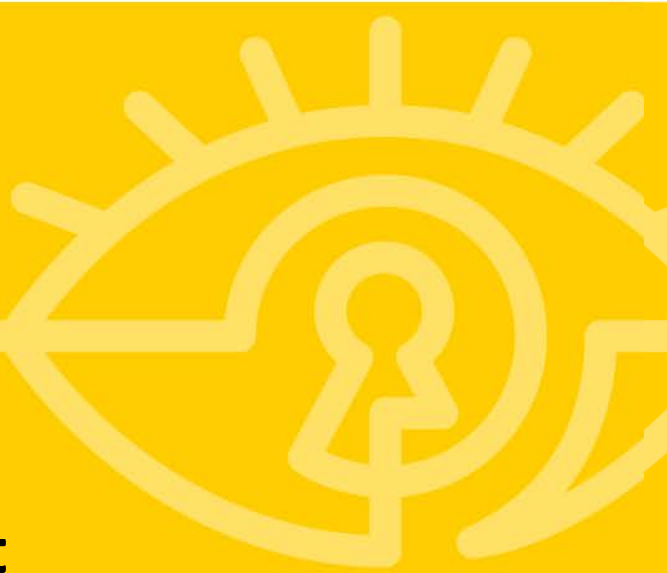
The Framework establishes a common language for cybersecurity



We also need a common language to help normalize and optimize activities

- Goal: Comply once – use many
- NIST identified > 450 commonly used standards & practices
- Many of these share categories and families of controls in common
- Keeping up with multiple compliance frameworks is resource intensive and costly
- Need to express requirements and status to supply chain partners

For example:
NIST SP 800-53 Control AC-3,
ISO 27002:2013 A.9.4.1, and
IEC 15408 FDP_ACC.2 all point to "**access control**" processes



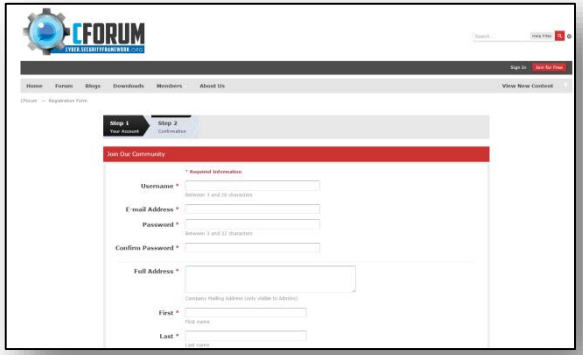
CSF Steps 3 and 4
Current Profile and Risk Assessment

CForum is an online forum for sharing lessons learned and good practices

- Industry leaders such as Tony Sager and Mike Brown help spark security conversations
- Several hundred users help ensure a balanced approach
- Relevant topic areas include:
  - Framework specific training and discussion
  - Topics for individual critical information sectors
  - Next iteration of the Framework
  - Implementation Guidance
  - Supply Chain Risk Management

CForum is a free online community bringing all sectors together

- Users can join for free to share experiences and ask questions
- Users can take advantage of the examples and lessons learned posted by others



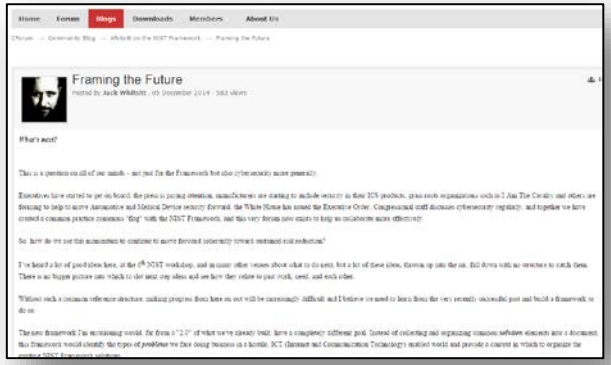
- Federal agencies are jump starting but aren't the long-term solution – governance will eventually transfer to "Industry"
- Assist industry in owning and leading cybersecurity management practices

CForum Members Responded to the 2015 NIST Request for Information

- CForum members are some of the most CSF-informed participants in the nation.
- The Forum requested feedback on several aspects of CSF usage, update and governance:
  - Components that are/are not useful?
  - Additions, changes or removals?
  - Improvements to CSF information sharing?
  - Private sector's involvement in future CSF governance?
  - Transitioning some/all of CSF coordination?
  - How to evaluate whether the transition partner has capacity to work effectively with domestic/intl organizations and governments?

Join cybersecurity and industry experts

- Experts in cybersecurity are invited to blog
- Sector specific blogs share relevant information
- Online collaboration provides access to industry leading experts



- A central locations for identifying best practices and guidance on cybersecurity
- Share your challenges to help others avoid similar pitfalls

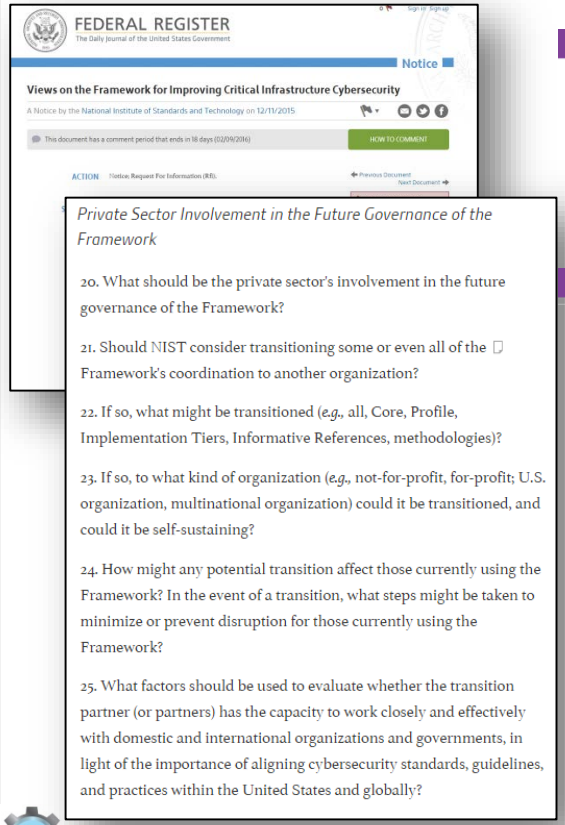
CSF Steps 5 through 7
Target Profile, Gap Analysis and Action Plan

Improve Security for the Community by leveraging shared templates

Function	Category	Subcategory	Priority	Org Policy	Org Practices	Status	Comments / Evidence
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	M				
		ID.AM-2: Software platforms and applications within the organization are inventoried	L				
		ID.AM-3: Organizational communication and data flows are mapped	H				
		ID.AM-4: External information systems are catalogued	M				
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on	M				
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party	H				

- Why re-invent the wheel?
- Take advantage of lessons learned by others
- Jump start use of cybersecurity resources by using shared templates
- Identify opportunities for consistency within and across critical infrastructure sectors

Industry leading the evolution of the Cybersecurity Framework



- Our target is for CForum to represent a consortium of security professionals and owner/operators across multiple industries
- CForum members and organizations helping to implement:
  - Private sector's involvement
  - CSF Governance
  - Criteria for participation and for providing industry resources

CFORUM
CYBER.SECURITYFRAMEWORK.ORG

Assessing the Gaps and the Road Ahead

- The current forum has hundreds of participants but very few are active – we need more voices asking more detailed questions.
- If the site is to provide value, we need more organizations providing anonymized examples of use.
- This is a community opportunity – if we want to continue to have a voice in the continued CSF evolution, we need to share our vision and experience.

Action Plan Based on Roadmap

- Now that you know where CForum has been and where it's going, we hope that you will join the conversation within the next week.
- Within three months, share information about how CSF is helping to improve communication in your organization.
- Within six months, your organization can be demonstrating your leadership and vision as you post profiles, informative references and/or sample action plans.

We are available if you have additional questions

Greg Witte
Senior Security Engineer
Greg.Witte @G2-inc.com
(301) 346-2385

Tom Conkle
Cybersecurity Engineer
Tom.Conkle@G2-inc.com
(443) 292-6679