Regulatory Harmonization
FSSCC Cybersecurity Profile

- An Overview -

Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

An Executive Summary:
The Issue the Profile Addresses, Its Development as a Solution, Its Benefits, and Support

The Issue: Domestic and international regulatory agencies asking the same question in many different ways, stretching already scarce cybersecurity talent.

The Profile as a Solution: The Profile, which is a common, standardized approach that can act as a baseline for examination and future cyber regulation - *fill out once per exam cycle, report out many*.

Voluntary with Many Benefits, Including:

- Provides more consistent and efficient processing of examination material by both firms and regulators.
- Allows Regulators and Firms to focus on systemic risk and risk residual to firms.
- Establishes an Industry best practice beyond regulatory use.

Supporting Associations:

FSSCC Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security

American Bankers Association

bpi Business Innovation Technology Security BITS

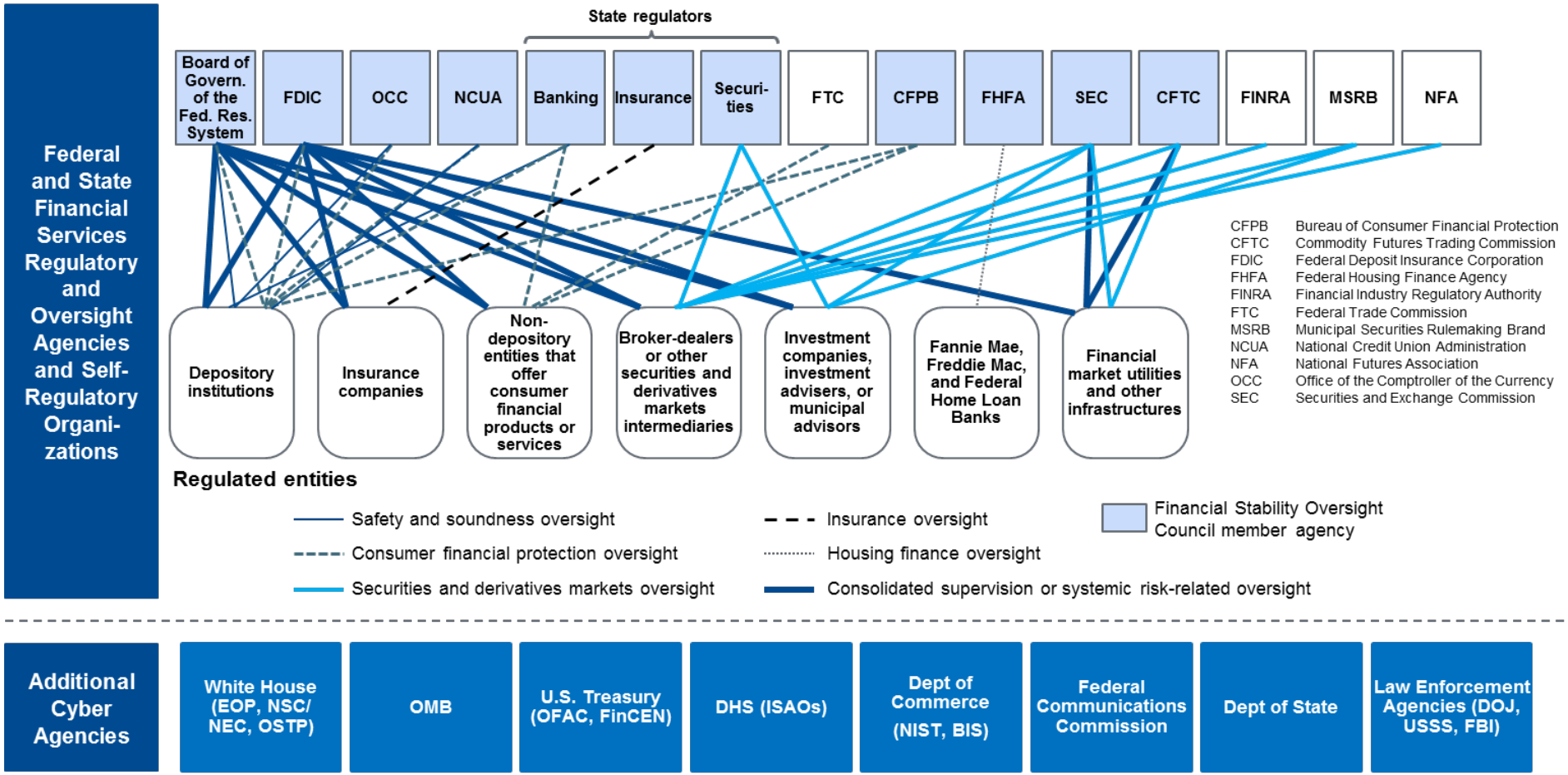
FIA

gfma

iib Institute of International Bankers Advancing the interests of the International Banking Community in the United States www.iib.org

IIF Institute of International Finance

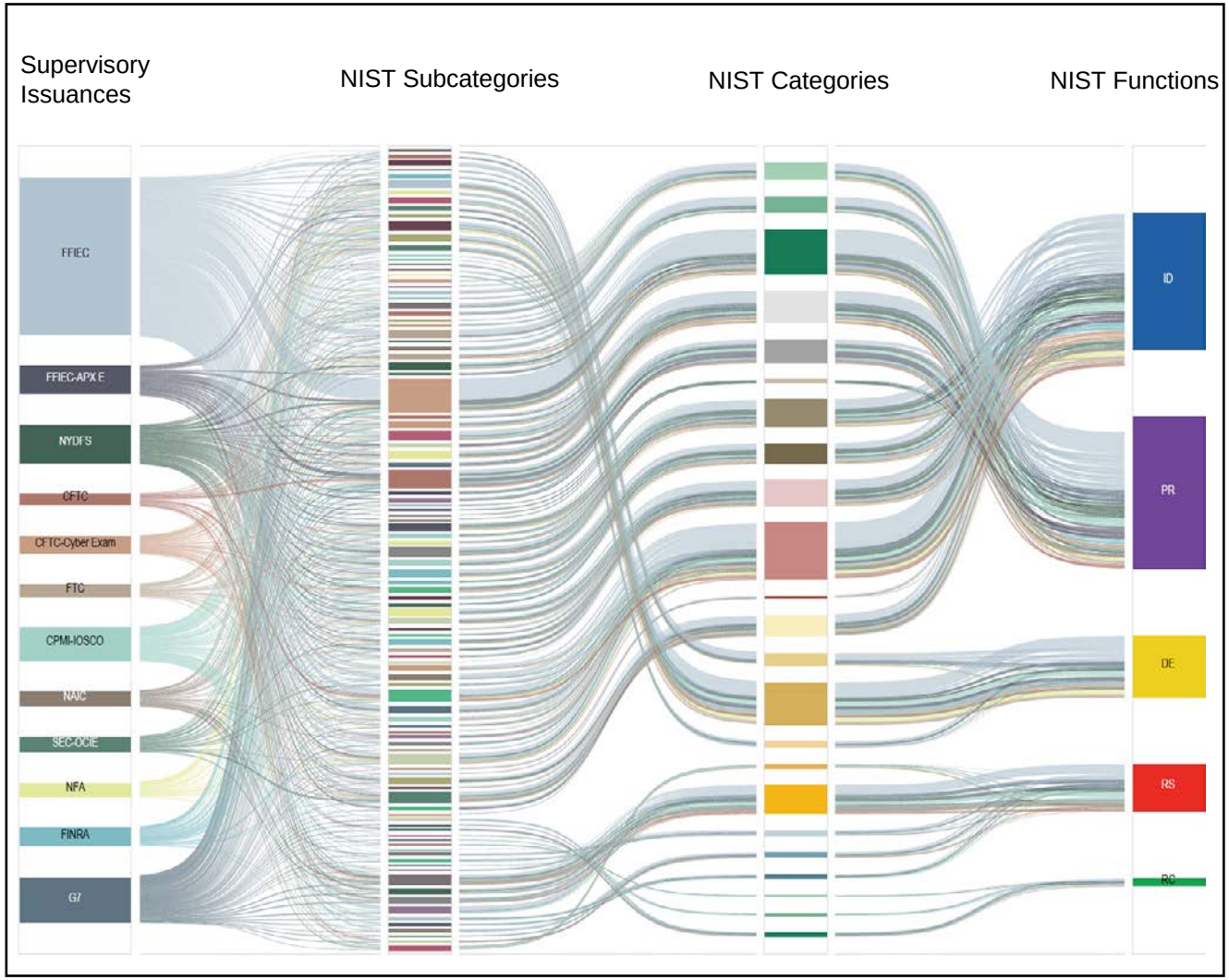
The U.S. Financial Services Regulatory Structure (2019)



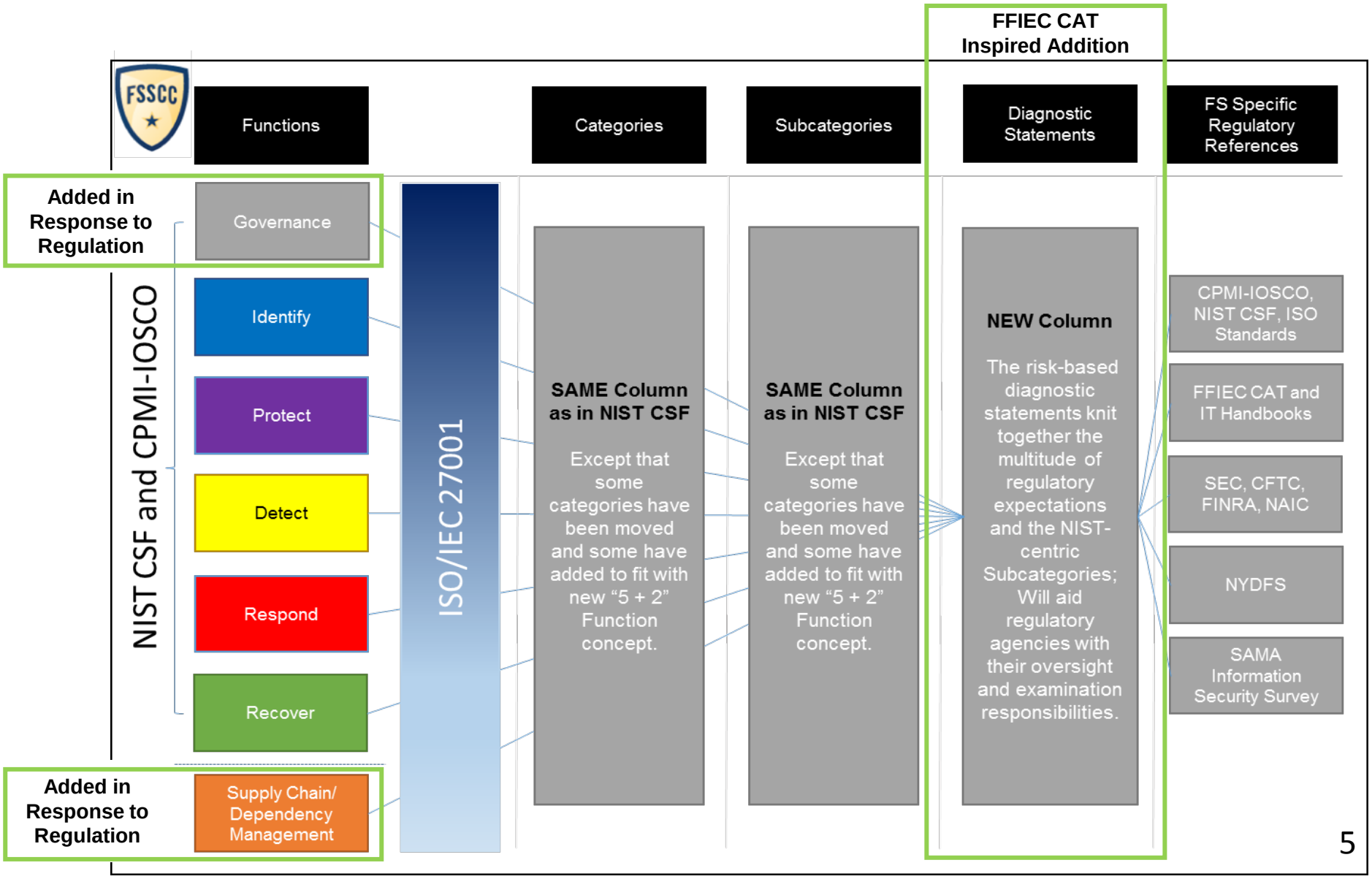
Note: The figure depicts the primary regulators in the US financial regulatory structure, as well as their primary oversight responsibilities. "Regulators" generally refers to entities that have rulemaking, supervisory, and enforcement authorities over financial institutions or entities. There are additional agencies involved in regulating the financial markets and there may be other possible regulatory connections than those depicted in this figure
Source: GAO; GAO-16-175

Topical Overlaps, Semantic Differences Lead to Time Spent on Reconciliation

- 2016 Survey: **40%** of Information Security teams' time on avg spent on reconciliation of cyber expectations
- (ISC)2: Gap of cyber pros has been growing, with a **gap of 3 million projected for 2019**
- FSB (2018): **72% of jurisdictions** reported plans to issue new cyber requirements



The Profile's Underlying Architecture



The Profile: A NIST Cybersecurity Framework Extension to Align with Financial Services Requirements and Supervisory Expectations

NIST Cybersecurity Framework provides a globally accepted organizational structure and taxonomy for cybersecurity and cyber risk management

The following countries are either exploring its use or promoting it through translation –

- Bermuda
- Brazil
- Canada
- Israel
- Italy
- Japan
- Malaysia
- Mexico
- Philippines
- Saudi Arabia
- Switzerland
- United Kingdom
- Uruguay

The Profile extends the NIST Cybersecurity Framework to be more inclusive of financial services requirements and supervisory expectations

Extended NIST to highlight 2 special categories of particular (& appropriate) regulatory focus:

The following international governments and organizations have expressed positive interest in the Profile –

- Argentina
- Brazil
- China (Mainland and Hong Kong)
- Chile
- European Union
- International Standards Organisation
- Japan
- Singapore
- United Kingdom

Benefits of the Profile Approach

Financial Institutions

- ✓ ***Optimization of cyber professionals' time*** "at the keyboard," defending against next gen attacks – ***complete once per cycle, report out to many***.
- ✓ ***Improved Boardroom and Executive engagement***, understanding and prioritization.
- ✓ Enhanced, ***efficient third-party vendor management***.

Supervisory Community

- ✓ ***Examinations more tailored to institutional complexity, enabling "deeper dives"*** in those areas of greater interest to that particular agency.
- ✓ ***Enables supervisory agencies to better discern the sector's systemic risk***, with more agency time for specialization, testing and validation.
- ✓ Enhanced ***visibility of non-sector and third-party cyber risks***.

The Ecosystem

- ✓ ***Based on NIST and ISO, it allows for greater intra-sector, cross-sector and international cybersecurity collaboration and understanding***.
- ✓ Enables ***collective action to better address collective risks***.
- ✓ ***Greater innovation as technology companies, including FinTech's, are able to evidence security*** against the standardized set of compliance requirements.

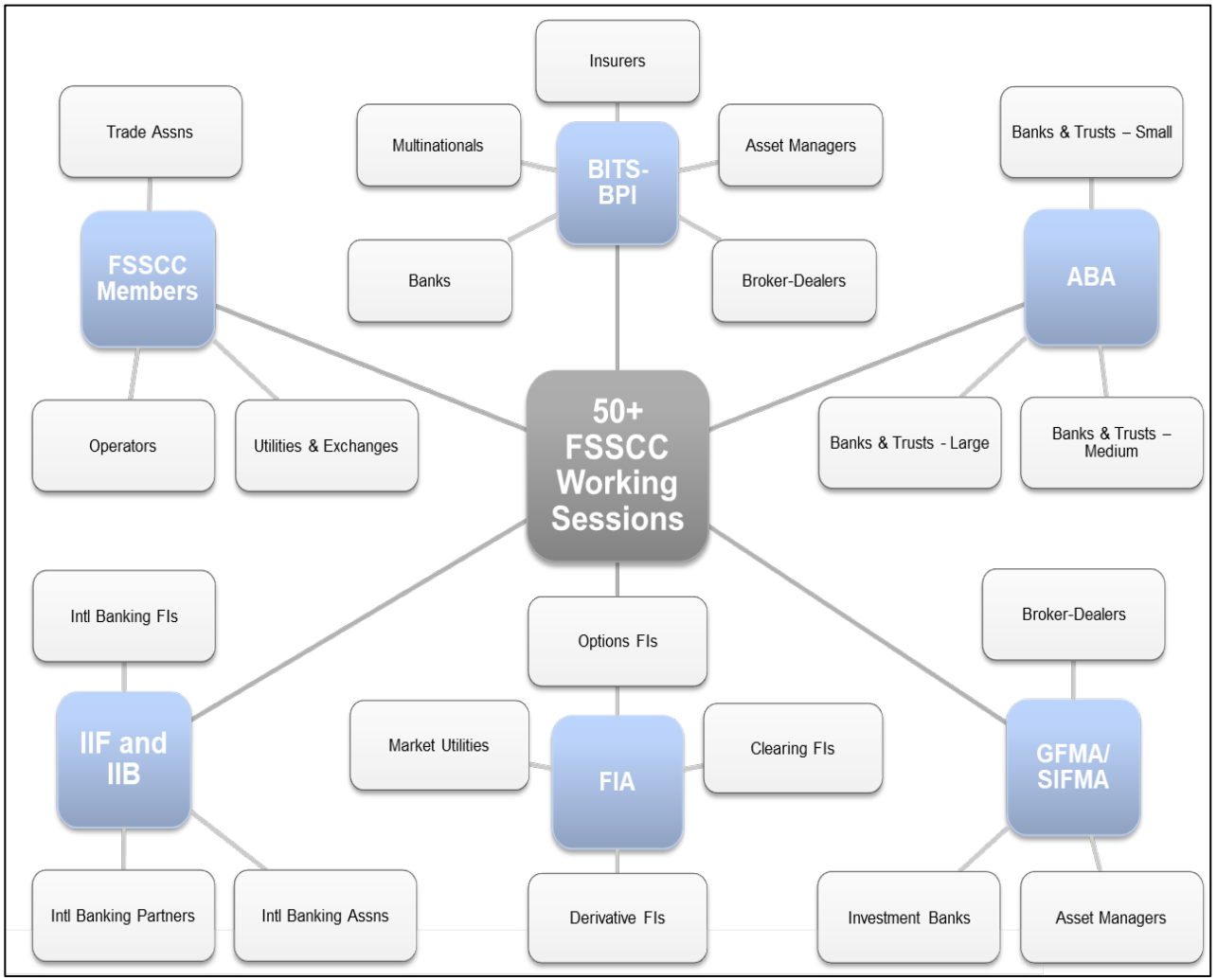
Developing the Profile: The Process and Main Participants

Over the past 2 years –

- Coalition under the FSSCC established;
- BITS and ABA co-lead;
- ***50+ working sessions;***
- ***300+ individual experts participated;***
- ***150+ financial institutions of all types provided input***.

Financial Services and Other Agencies –

- *Provided material for incorporation*, notably:
  - FRB;
  - OCC;
  - FDIC;
  - SEC;
  - CFTC;
  - FINRA;
- Facilitated a NIST workshop on risk/impact scaling.



Public/Private Collaboration to Achieve Sector-Wide Scaling by Impact

National or Global Impact – Tier 1

- Applies to systemically important and/or multinational firms.
- Examples: GSIBs, GSIFIs, systemically important market utilities.

Subnational (Regional) Impact – Tier 2

- Applies to firms offering mission critical services or have over 5m customer accounts.
- Examples: Super-regional banks, significant portion of large insurance firms.

- Industry-wide scaling achieved through collaboration with NIST, Federal Reserve, OCC, FDIC, SEC, FINRA.

- Over 40 firms implementing the Profile or actively exploring implementation for 2019/2020.

- Applies to firms with a high degree of interconnectedness and between 1-5 customer accounts.
- Examples: Regional banks, large credit unions.

Sector Only Impact – Tier 3

- Applies to the firms with a relatively small number of customers.
- Examples: Community banks, small broker dealers/investment advisors.

Customer/3rd Party Impact Only – Tier 4

Documented Agency Statements of Support

- **FFIEC:** "…These resources are actionable and help financial institutions manage cybersecurity risk regardless of whether they use the FFIEC Cybersecurity Assessment Tool, NIST Cybersecurity Framework, Financial Services Sector Specific Cybersecurity Profile, or any other methodology to assess their cybersecurity preparedness."

- **NIST:** "…[O]ne of the more detailed Cybersecurity Framework-based, sector regulatory harmonization approaches to-date."

- **Federal Reserve:** "… we'll welcome any financial institution to provide information to us using the structure and taxonomy of the profile, we see that as a boon for harmonization."

- **OCC:** "If the industry moves to use this cybersecurity profile, that is what we will base our assessments on…."

- **FDIC:** "That was one of the things, at the FDIC, that we were most interested in is looking at the tiering."

- **SEC:** "…to the extent that we can rationalize and cut down on that duplication, allowing those scarce resources to start driving toward protecting the enterprise, I think we're in a good space."

Regulatory Harmonization through the Profile: The Sector's Requests

To maximize the benefits of the Profile for both financial institutions and supervisory agencies alike, we encourage the following –

- Public statements of support (similar to the one on the prior slide) stating that use of the Profile as input for examinations (and as the mechanism to evidence compliance) is acceptable.
- Support the Profile as a common baseline framework for cyber supervision in conversations within the FBIIC and with international regulators.

Websites

- https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile
- https://www.fsscc.org/The-Profile-FAQs
- https://www.fsscc.org/files/galleries/NIST_Letter_of_Support_re_FSSCC_Financial_Services_Sector_Cybersecurity_Profile.pdf

Appendix:
A Visual Example of the Tiering and Diagnostic Statements

A More Granular View The Profile identifies key attributes of a cybersecurity program and articulates them in a consistent manner through suggested diagnostic statements and references to international standards and best practices. The Profile can be leveraged to respond consistently to multiple supervisory requests.

Functions	Categories	Subcategories	NIST CSF v1.1 Ref	FS Profile Diagnostic Statements	Diagnostic Statement Reponses	Tier 1: National+	Tier 2: Sub-National	Tier 3: Sector	Tier 4: Localized	FS References	Informative References from NIST CSF v1.1
Governance	**Strategy and Framework (GV.SF):** The organization has a cyber risk management framework that is reviewed and approved by the Board and is informed by the organization's risk tolerances and its role in critical infrastructure.	**GV.SF-1:** Organization has a cyber risk management strategy and framework.	ID.BE-3; ID.RM-1 - with sector enhancement	GV.SF-1.3: The organization's cyber risk management strategy identifies and documents the organization's role as it relates to other critical infrastructures outside of the financial services sector and the risk that the organization may pose to them.	❑ Yes ❑ No ❑ Partial ❑ Not Applicable ❑ Yes – Risk Based ❑ Yes – Compensating Controls ❑ Not Tested ❑ I Don't Know					CPMI-IOSCO, FFIEC/1, FINRA, FFIEC IT Booklet/Information Security/I, FFIEC IT Booklet/Management/I.B, FFIEC IT Booklet/Operations	• COBIT 5 APO02.06, APO03.01 • ISO/IEC 27001:2013 Clause 4.1 • NIST SP 800-53 Rev. 4 PM-8
				GV.SF-1.4: The cyber risk management strategy identifies and communicates the organization's role within the financial services sector as a component of critical infrastructure in the financial services industry.	❑ Yes ❑ No ❑ Partial ❑ Not Applicable ❑ Yes – Risk Based ❑ Yes – Compensating Controls ❑ Not Tested ❑ I Don't Know					CPMI-IOSCO, FFIEC/1, FINRA, FFIEC IT Booklet/Management/I.A, FFIEC IT Booklet/Operations	
				GV.SF-1.5: The cyber risk management strategy and framework establishes and communicates priorities for organizational mission, objectives, and activities.	❑ Yes ❑ No ❑ Partial ❑ Not Applicable ❑ Yes – Risk Based ❑ Yes – Compensating Controls ❑ Not Tested ❑ I Don't Know					CPMI-IOSCO, FFIEC/1, FINRA, FFIEC IT Booklet/Information Security/I, FFIEC IT Booklet/Management/I, FFIEC IT Booklet/Operations	

The **'Diagnostic Statements'** column defines authoritative, common language for multiple regulatory requirements, enabling Firms to comply with largely the same but distinct requirements from different supervisors

The **'FS References'** and **'Informative References'** columns detail specific mapping of distinct requirements to the single Profile requirement

Appendix:
Benefits Explored - Efficiencies Gained

- ***73% Reduction for Community Institution Assessment Questions.*** For the least complex and interconnected institutions, it is expected that they would answer a total of 145 questions (9 tiering questions + 136 Diagnostic Statement questions). As compared to another widely-used assessment tool's 533 questions, this represents a ***73% reduction.***

- ***49% Reduction in Assessment Questions for the Largest Institutions.*** For the most complex and interconnected institutions, the reduction also is significant. With the Profile, it is expected that such institutions would answer 279 questions (2 tiering questions + 277 Diagnostic Statement questions) as compared to the other widely-used assessment's 533, ***a 49% reduction.***