The 28th National HIPAA Summit

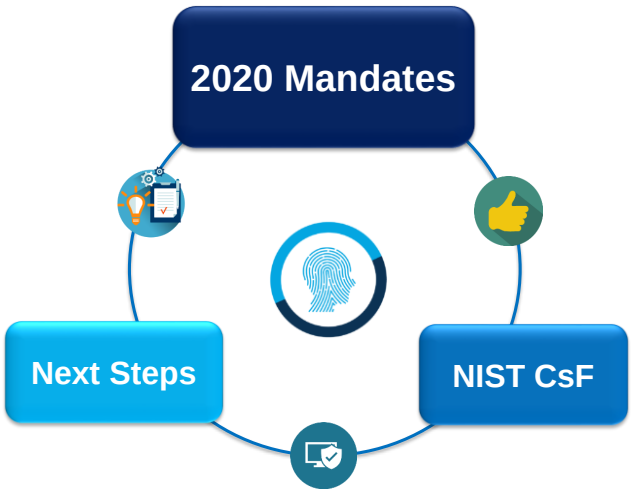
NIST CsF = Standard for HIPAA Compliance + Cybersecurity

Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP)
CCSFP (HITRUST), Member (FBI) InfraGard

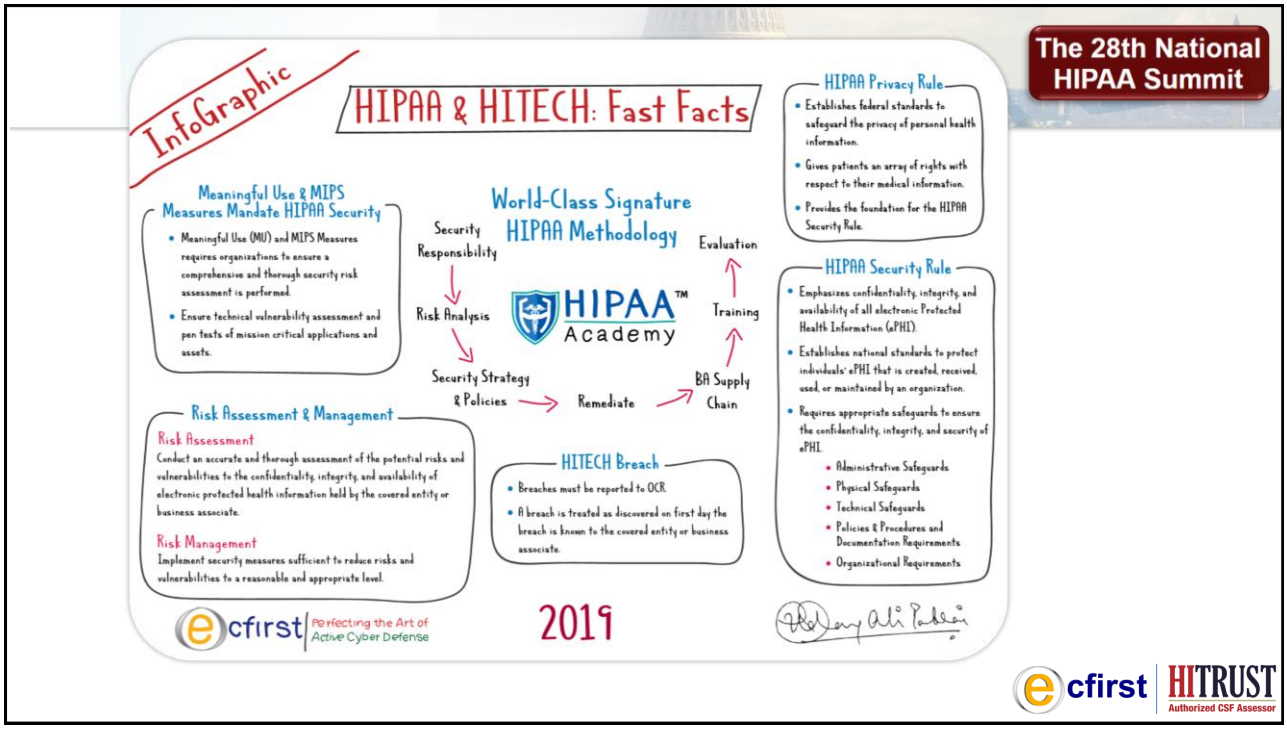
ecfirst | HITRUST Authorized CSF Assessor

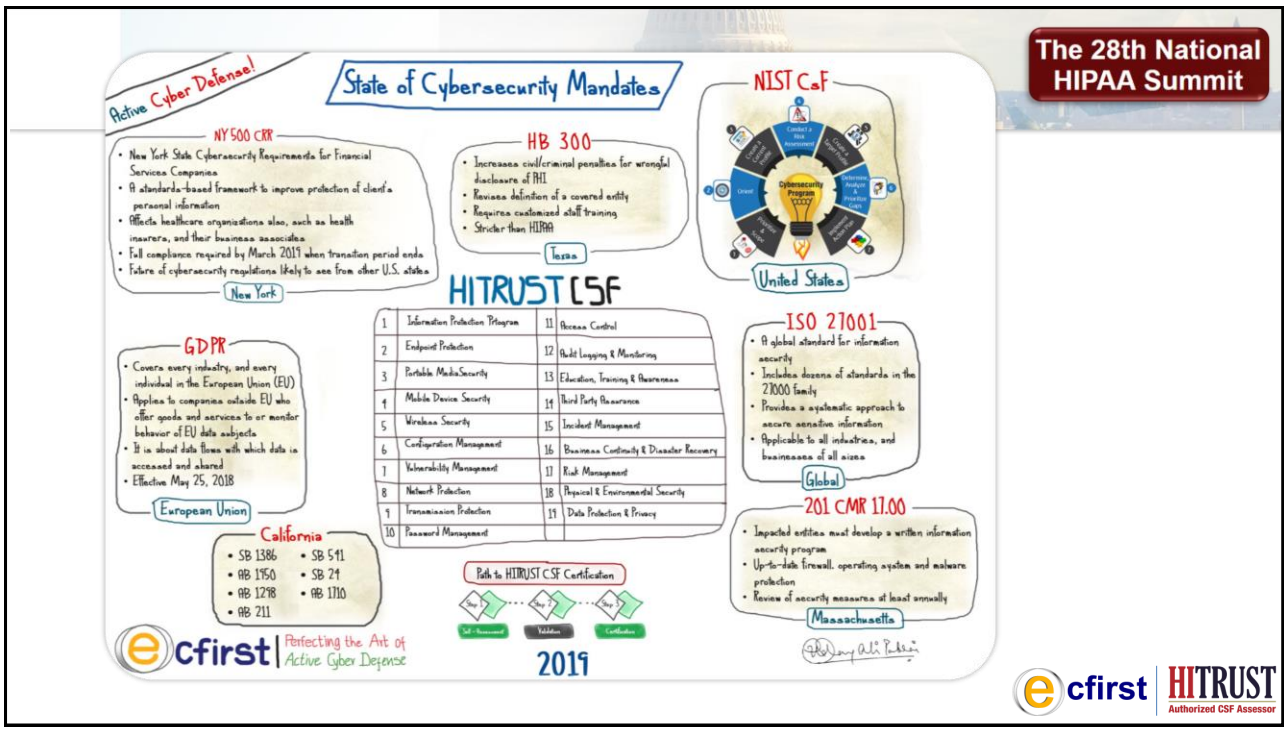
Agenda

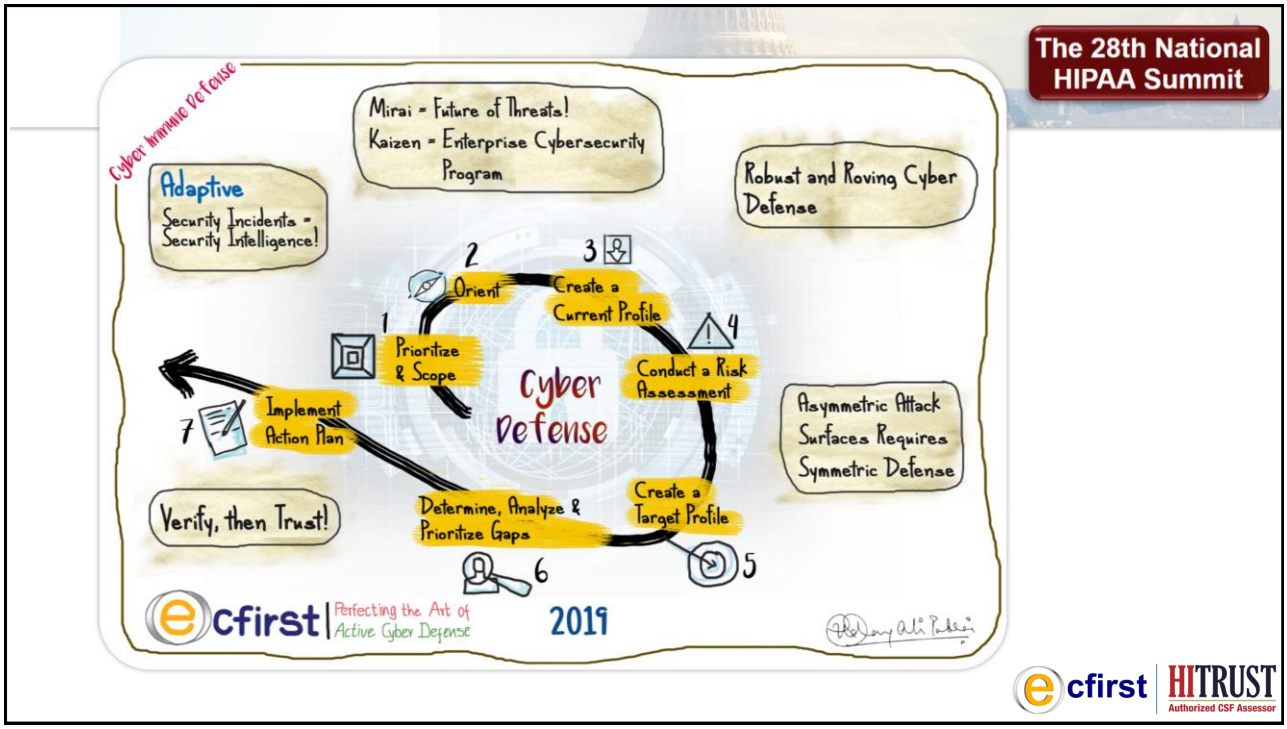
The 28th National HIPAA Summit

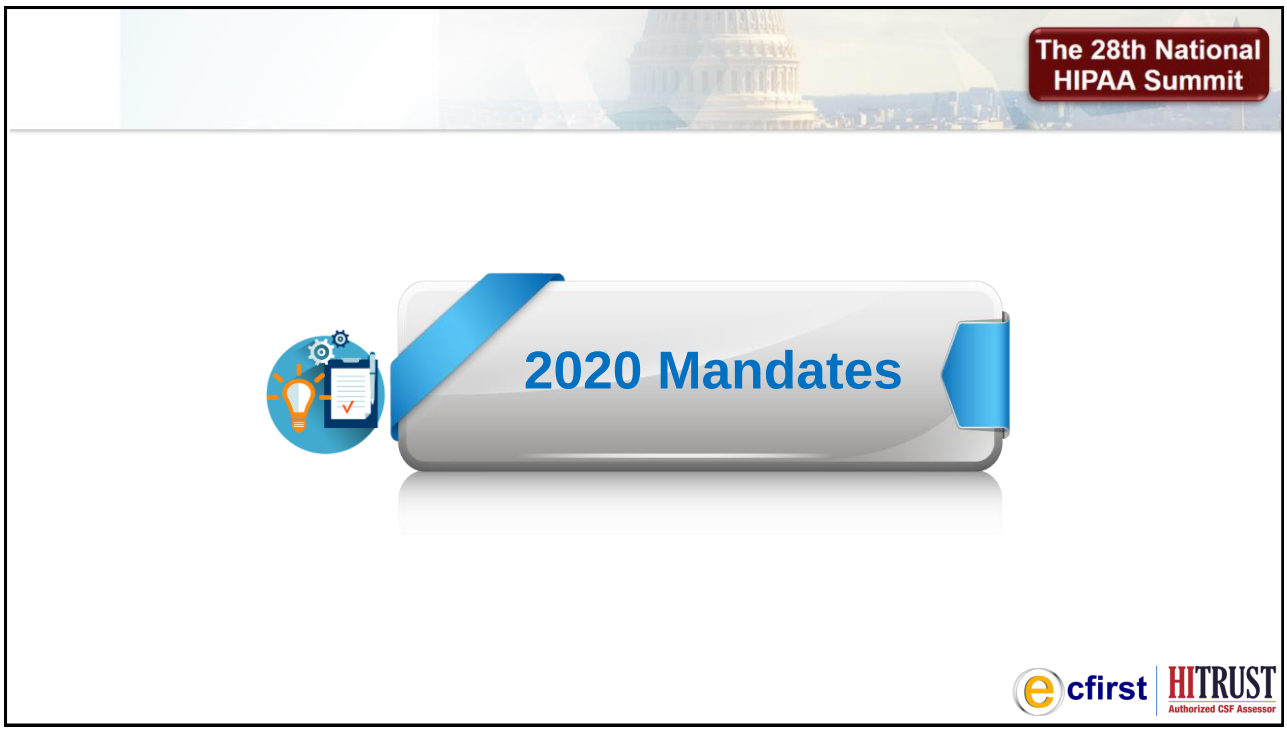


ecfirst | HITRUST Authorized CSF Assessor









SB 327 Information Privacy: Connected Devices

The 28th National HIPAA Summit

Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

- Effective **January 1, 2020**
- SB 327 requires manufacturers of connected devices to equip the device with reasonable security features that are appropriate to the nature and function of the device, appropriate to the information it may *collect*, *contain*, or *transmit*
- Designed to protect the device and any information contained therein from *unauthorized access, destruction, use, modification, or disclosure*

CALIFORNIA

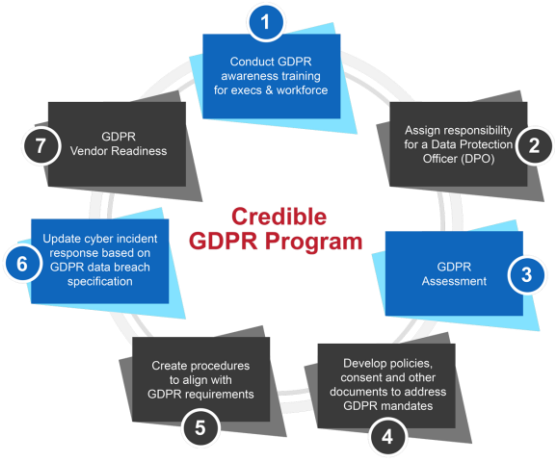
SB 327

IoT Security

ecfirst | HITRUST Authorized CSF Assessor

GDPR: European Standard
CCPA: California Impact

The 28th National HIPAA Summit



ecfirst | HITRUST Authorized CSF Assessor

California Consumer Privacy Act (CCPA)

The 28th National HIPAA Summit

CCPA grants California residents the right:

Effective **January 1, 2020**

- To know what personal information is being collected about them.
- To know whether their personal information is sold or otherwise disclosed and to whom.
- To say no to the sale of their personal information.
- To access their personal information and request deletion under certain circumstances.
- To receive equal service and price, even if they exercise their privacy rights.

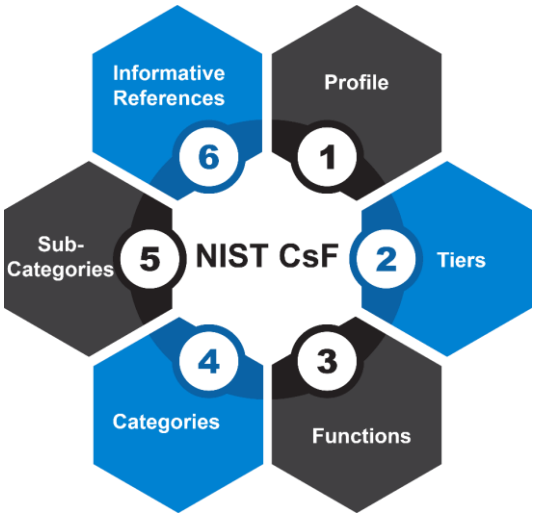
ecfirst | HITRUST Authorized CSF Assessor

The 28th National HIPAA Summit

ecfirst | HITRUST Authorized CSF Assessor

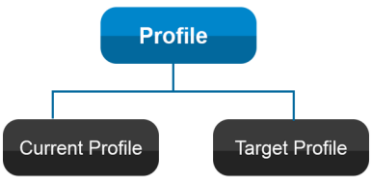
NIST CsF

The 28th National HIPAA Summit



NIST CsF: Organization

The 28th National HIPAA Summit



Profile

Tiers

Functions

Function and Category Unique Identifiers

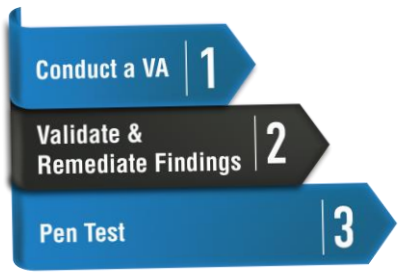
The 28th National HIPAA Summit

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

ecfirst | HITRUST Authorized CSF Assessor

Enterprise Risk Assessment

The 28th National HIPAA Summit



ecfirst | HITRUST Authorized CSF Assessor

NIST CSF/HIPAA Mapping

The 28th National HIPAA Summit

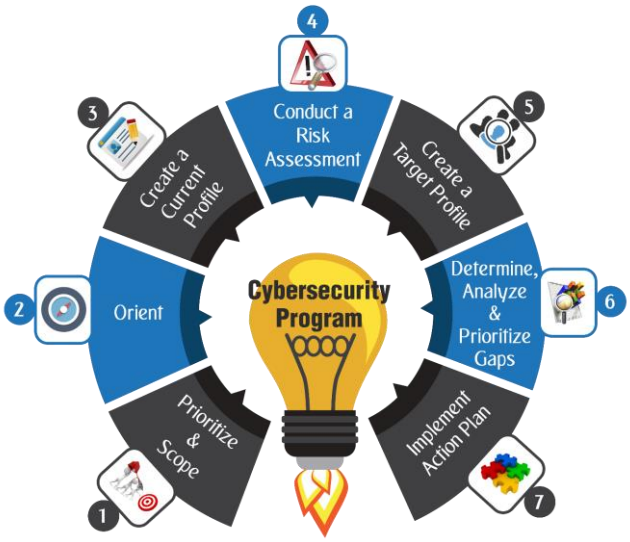
#	NIST CsF v1.1 Controls Mapping	HIPAA Security Rule Standards & Implementation Specifications
Identify (ID)		
1	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC
		164.310(a)(2)(ii) Facility Security Plan (A) SPEC
		164.310(d)(1) Device and Media Controls SPEC
2	**ID.AM-2:** Software platforms and applications within the organization are inventoried.	164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC
		164.308(a)(7)(ii)(E) Applications and Data Criticality Analysis (A) SPEC
3	**ID.AM-3:** Organizational communication and data flows are mapped.	164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC
		164.308(a)(3)(ii)(A) Authorization and/or Supervision (A) SPEC
		164.310(d)(1) Device and Media Controls SPEC
4	**ID.AM-4:** External information systems are catalogued.	164.308(a)(4)(ii)(A) Isolating Health Care Clearinghouse Function (R) SPEC
		164.308(b)(1) Business Associate Contracts and Other Arrangements SPEC
		164.314(a)(1) Business Associate Contracts or Other Arrangements STD
		164.314(a)(2)(i) Business associate contracts SPEC
		164.314(a)(2)(ii) Other arrangements SPEC
		164.316(b)(2)(i) Time Limit (R) SPEC

ecfirst | HITRUST Authorized CSF Assessor

HIPAA Cybersecurity Program

The 28th National HIPAA Summit

NIST CsF



ecfirst | HITRUST Authorized CSF Assessor

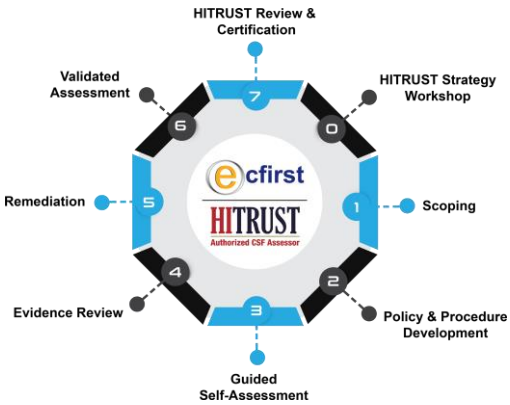
The 28th National HIPAA Summit

Next Steps

ecfirst | HITRUST Authorized CSF Assessor

HITRUST + NIST Certification

The 28th National HIPAA Summit



HITRUST / NIST Certification Roadmap

Establish a Credible HIPAA Program!

ecfirst | HITRUST Authorized CSF Assessor

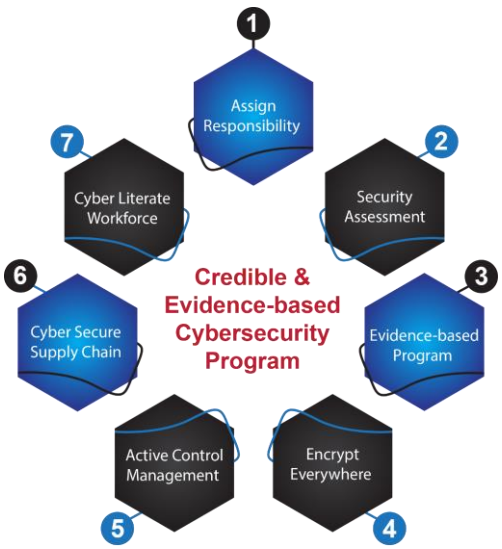
HIPAA Cybersecurity Program:
Five Dimensions Aligned

The 28th National HIPAA Summit

ecfirst | HITRUST Authorized CSF Assessor

Cyber Immune Defense

The 28th National HIPAA Summit



ecfirst | HITRUST Authorized CSF Assessor

Cyber Action Required Annually!

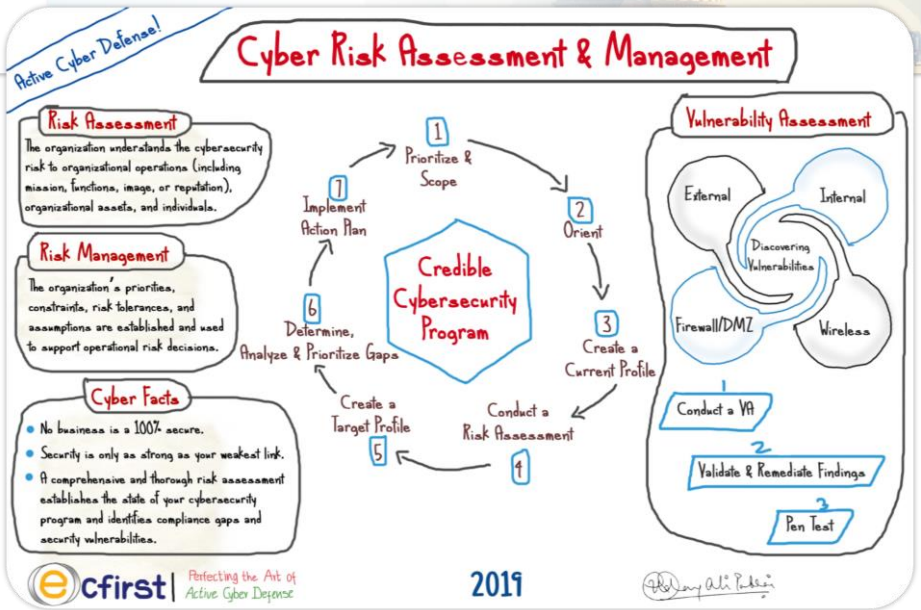
The 28th National HIPAA Summit

1. Develop a credible cybersecurity strategy
2. Conduct a comprehensive security risk assessment
3. Ensure a technical vulnerability assessment is performed quarterly, and a pen test annually
4. Perform a Business Impact Analysis (BIA)
5. Develop a detailed Disaster Recovery Plan (DRP)
6. Create a cyber incident response plan
7. Implement a cybersecurity framework (e.g. HITRUST, NIST CSF)

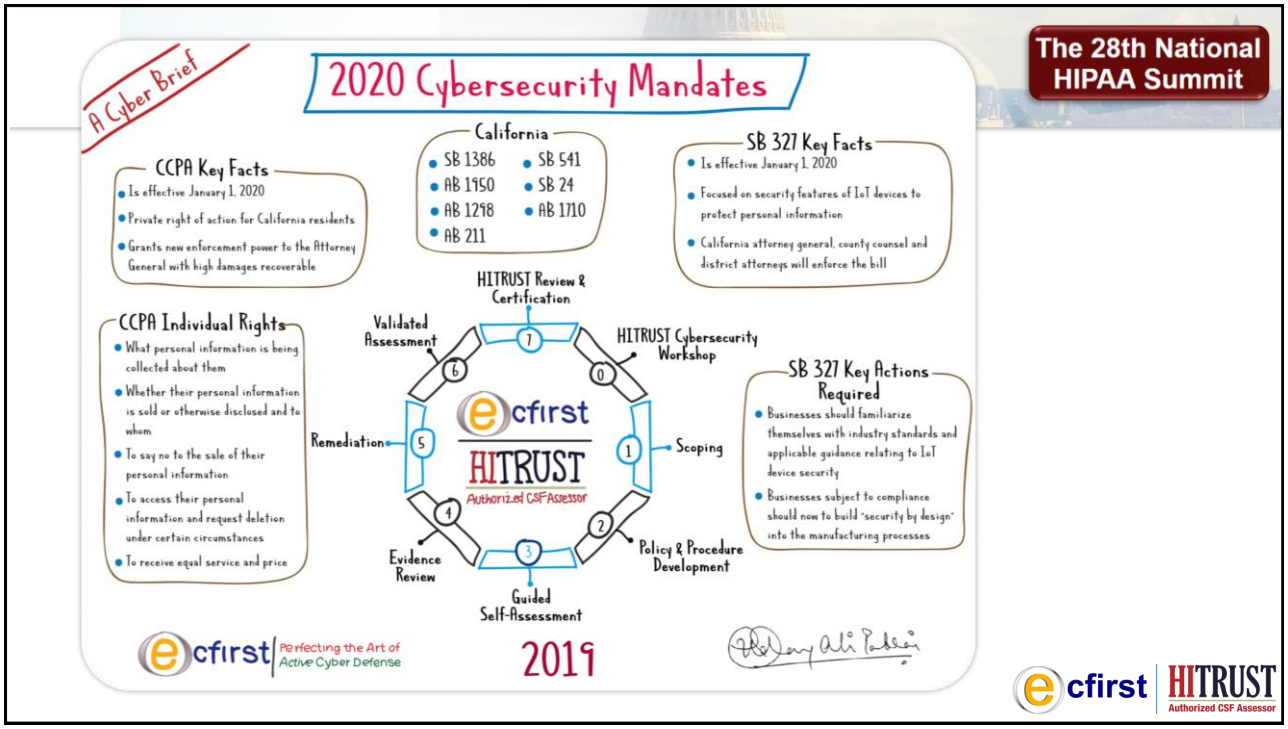
Lifecycle approach

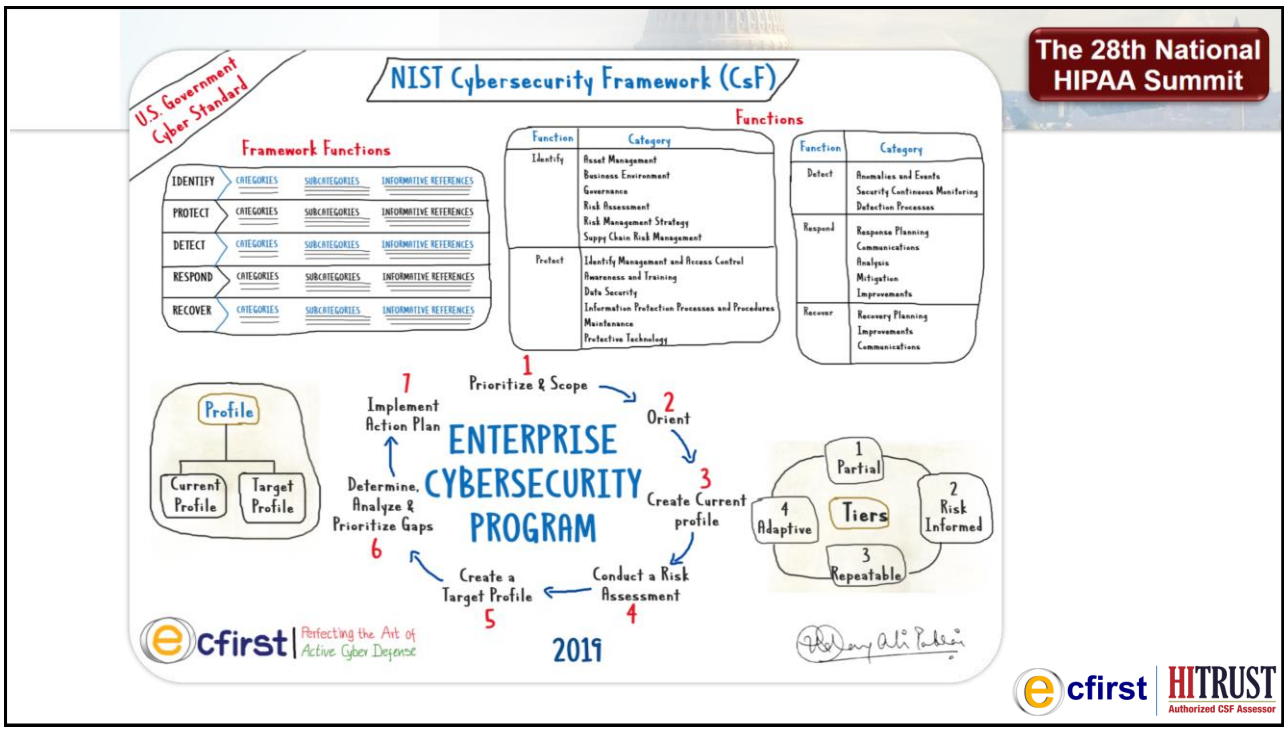
ecfirst | HITRUST Authorized CSF Assessor

The 28th National HIPAA Summit



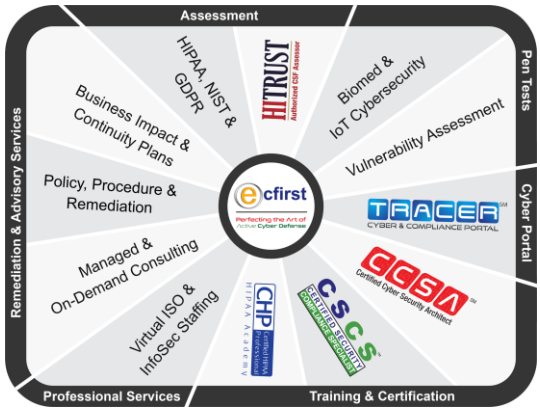
ecfirst | HITRUST Authorized CSF Assessor





About ecfirst

The 28th National HIPAA Summit



VISION (Mantra)

Enabling establishment of an active cyber defense program and capability.

MISSION (Karma)

Implement an evidence-based compliance program integrated within an enterprise-wide active cyber defense system.

OUR PROMISE

- Unconditional Guarantee. No Questions!
- ecfirst will not consider an engagement complete unless client is 100% satisfied.

Delivering Everything Compliance. Everything Security.
1000s of Clients | Clients in all 50 States | Clients on 5 Continents | HITRUST Authorized CSF Assessor

ecfirst | HITRUST Authorized CSF Assessor

Certification Training

The 28th National HIPAA Summit

- CHP Certified HIPAA Professional — HIPAA Academy — **Certified HIPAA Professional**
- CSCS Certified Security Compliance Specialist — **Certified Security Compliance Specialist™**
- CCSA Certified Cyber Security Architect — **Certified Cyber Security Architect℠**
- HITRUST Authorized CSF Assessor — **HITRUST Cybersecurity Strategy Workshop**

ecfirst | HITRUST Authorized CSF Assessor

Thank You!

The 28th National HIPAA Summit

+1.949.528.5224 | Ali.Pabrai@ecfirst.com

ecfirst | HITRUST Authorized CSF Assessor