CSG

CSG 2020 OCT. 26-DEC. 18
National Conference
REIMAGINED

Privacy & Cybersecurity Policy Academy

Dec. 7 | 1-5 p.m. ET

CSG

CSG 2020 National Conference REIMAGINED

OCT. 26-DEC. 18

THANK YOU TO THE 2020 NATIONAL CONFERENCE SPONSORS!

ACT®

AGA American Gas Association

alzheimer's association®

American® Chemistry Council

ANA AMERICAN NURSES ASSOCIATION

AHIP America's Health Insurance Plans

AT&T

Bio Biotechnology Industry Organization

CVSHealth

Consumer Technology Association™

EEI Edison Electric INSTITUTE

Lilly

esri®

EVERYTOWN FOR GUN SAFETY

gsk GlaxoSmithKline

GILEAD Creating Possible

CSG

CSG 2020 National Conference REIMAGINED

OCT. 26-DEC. 18

THANK YOU TO THE 2020 NATIONAL CONFERENCE SPONSORS!

HAWTHORNE™

HCA Healthcare℠

INTERNATIONAL PAPER

LexisNexis State Net®

LIFEPOINT HEALTH

McKESSON

Microsoft

novo nordisk®

Pfizer

PHILIPS

PhRMA RESEARCH • PROGRESS • HOPE

SANOFI

sunovion Innovation today, healthier tomorrows

Teladoc™ HEALTH

WGU®

CSG

CSG 2020 OCT. 26-DEC. 18
National Conference
REIMAGINED

Housekeeping

This presentation is being recorded. The recorded presentation will be posted to *web.csg.org/2020* on the Monday following the session. If you have questions, contact **registration@csg.org.**

To reduce noise during the presentation, all participants will be muted. If you have questions or comments, please utilize the **"Raise Your Hand"** functions or place your question in the **Chat.** Speakers may take questions throughout or at the end.

Captioning is provided during this session. To activate, select the CC option in the Zoom menu below and turn on subtitles.

If you have technical difficulties or if you have a question about Zoom or any of these instructions, please use the **Chat** feature in your menu to type a question. CSG staff will get back to you as soon as possible.

CSG

CSG 2020 National Conference REIMAGINED

OCT. 26-DEC. 18

Stacey Gray
Senior Counsel, Future of Privacy Forum

Sen. Hannah Beth Jackson
California

Sen. Joe Nguyen
Washington

Andrew Kingman
Senior Managing Attorney, DLA Piper

CSG 2020 OCT. 26-DEC. 18
National Conference
REIMAGINED

Break

Programming will resume shortly

CSG

CSG 2020 National Conference REIMAGINED

OCT. 26-DEC. 18

Nakia Grayson
IT Security Specialist, National Institute of Standards and Technology

Duane Schell
Chief Technology Officer, North Dakota

Fielding Greaves
Senior Director of State and Regional Government Affairs, AvaMed

Quentin Palfrey
President, International Digital Accountability Council

National Cybersecurity Center of Excellence

Privacy Integration in Securing Telehealth Remote Patient Monitoring Ecosystem

CSG Virtual Policy Academy — Privacy and Cybersecurity

December 7, 2020

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

NCCoE Securing Telehealth RPM Project

- ***Challenge*** *- prevent misuse or compromise of patient's data within an interconnected ecosystem (HDO's, telehealth platform providers, and patients)*
- ***Goal*** *- to provide a practical solution for securing the telehealth RPM ecosystem*
- ***Risk based approach*** *based on NIST Cybersecurity Framework and industry standards and best practices, including NIST Privacy Framework*
- ***Reference architecture*** *design with desired security capabilities*
- ***Build*** *a practical, usable, repeatable implementation to address the cybersecurity challenge*
- ***Result*** *in a freely available NIST Special Publication 1800-series Cybersecurity Practice Guide.*

SP 1800 Series: Cybersecurity Practice Guides

Volume A: Executive Summary

- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

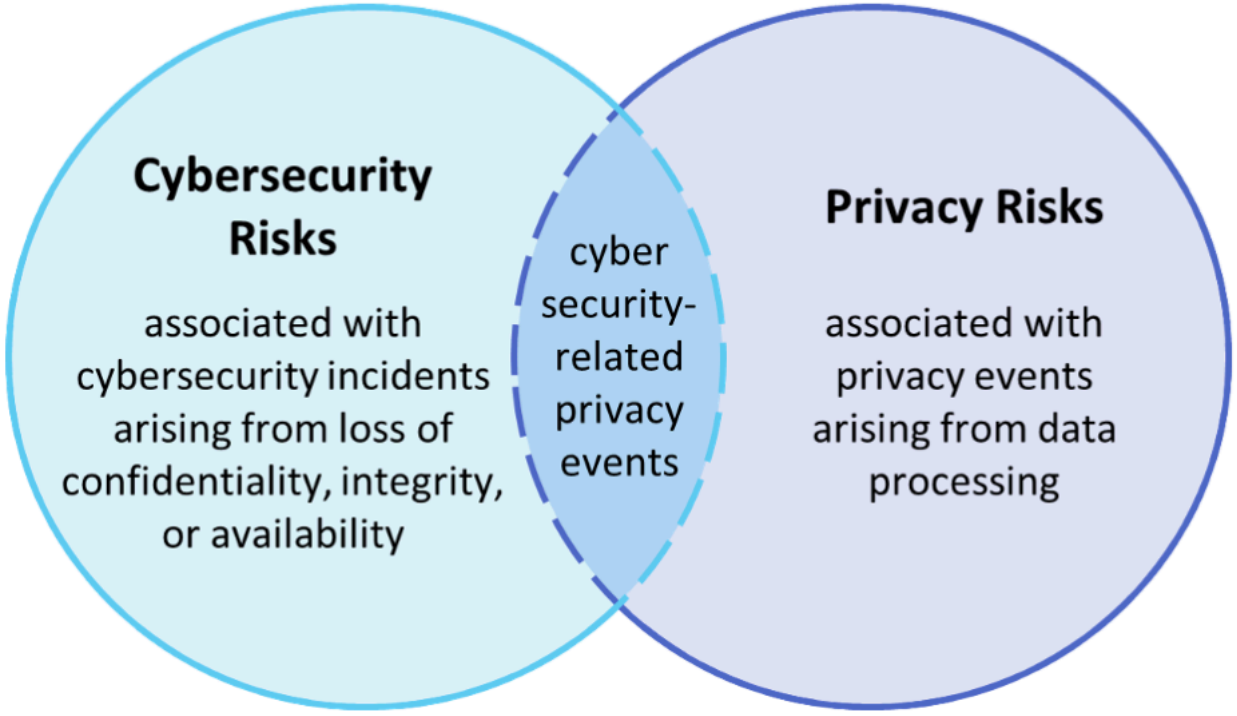
- Deep dive into challenge and solution, including approach, architecture, and security mapping to the NIST Cybersecurity Framework and other relevant standards, including the NIST Privacy Framework

Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

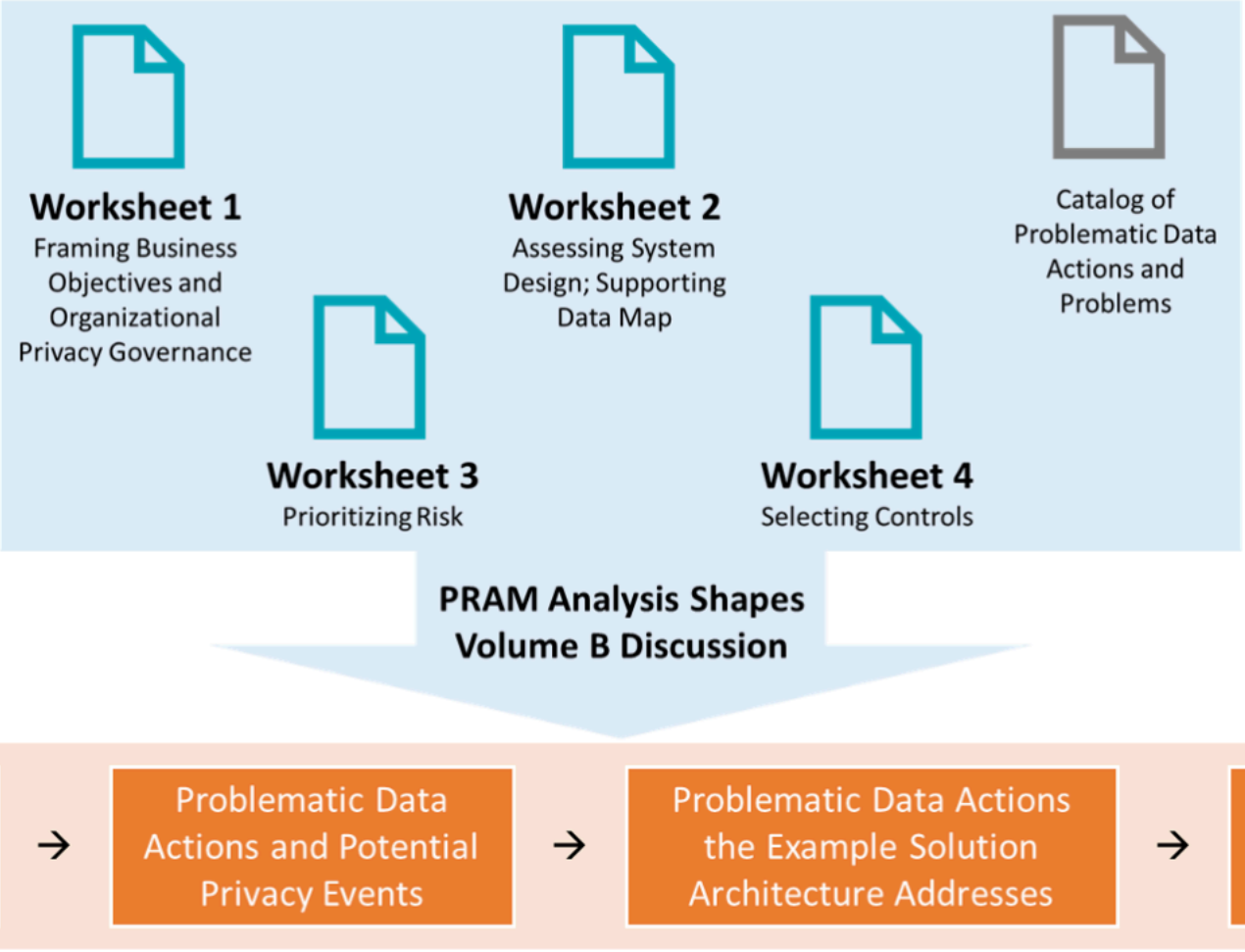
Addressing Privacy

- **Objectives**
  - Highlight the importance of privacy in this context
  - Identify areas where the solution addresses privacy risk
- **Approach**
  - NIST Privacy Risk Assessment Methodology (PRAM) analysis to identify potential problems for individuals
  - NIST Privacy Framework and controls mapping (technologies / privacy capabilities)



Source: *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, January 16, 2020.*
https://www.nist.gov/privacy-framework

NIST PRAM



Solution Data Actions (Operations/Flows) → Problematic Data Actions and Potential Privacy Events → Problematic Data Actions the Example Solution Architecture Addresses → Supporting Technologies/ Products

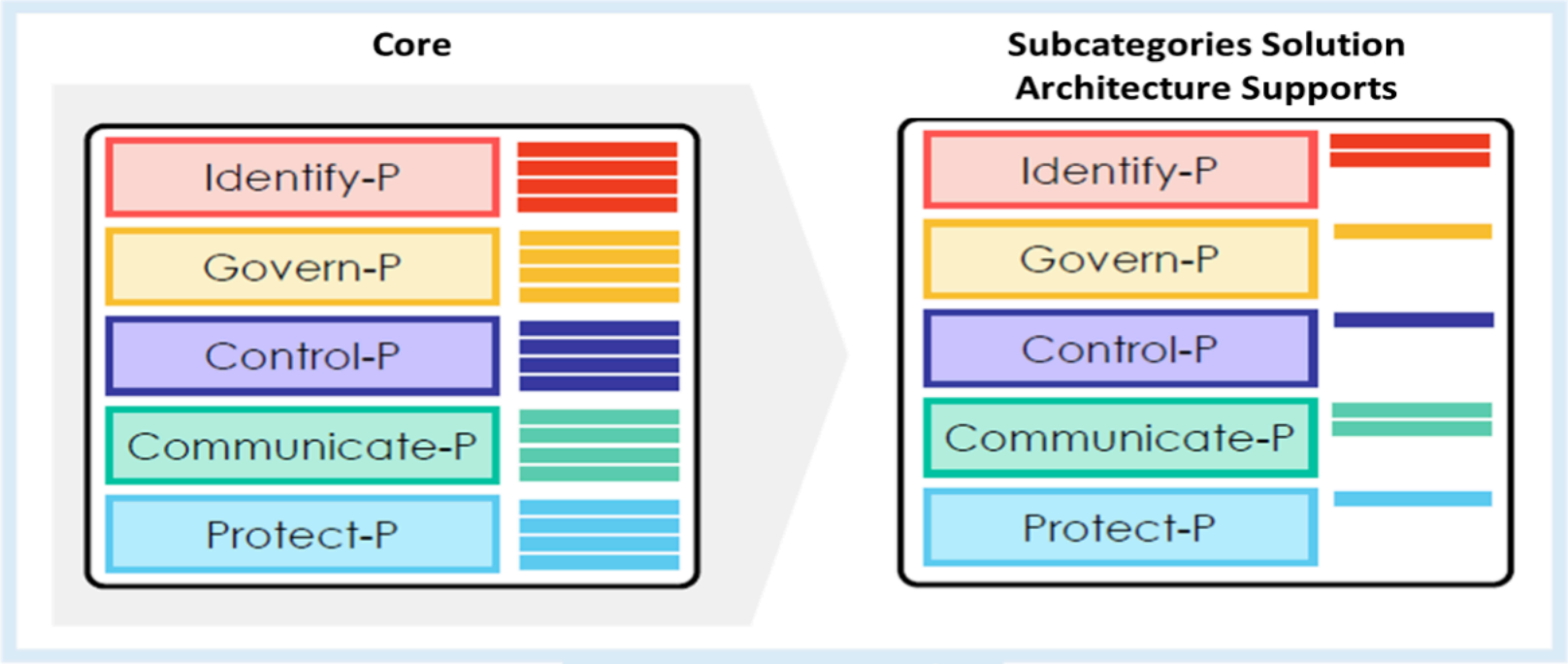
Potential Privacy Events

Problematic Data Action (PDA) ID	Data Actions	Problematic Data Actions and Example Privacy Events	How the Example Solution Architecture Helps Mitigate the PDA	Additional Privacy Mitigations for Organizations to Consider	The Technology Function that Helps Mitigate the PDA
PDA-1: Unauthorized individuals may access data on devices	Patients' readings are taken from the biometric device and collected by the RPM mobile device and forwarded to the telehealth platform.	Insecurity: Data between all these devices may not be protected at rest or in transit. Data may include sensitive information. Disclosure of this sensitive information could cause harm to the patient.	Protect data at rest and in transit between devices and telehealth platforms.	Develop and adopt enterprise encryption policies.	Technology Solution 1 Technology Solution 2
PDA-2: Incorrect data capture of readings by devices	The RPM solution relies on the patient to take readings by using the patient's assigned biometric device(s).	Distortion: Devices may be inaccurately applied by the patient (e.g., not properly using or inadvertently changing settings) which can impact the ability of a biometric device to take proper readings.	Responsibility for monitoring patient data, including identifying anomalies, falls on the clinician.	Educate patients regarding practices for handling biometric device(s).	Technology Solution 3 Technology Solution 4

Potential Privacy Events

Problematic Data Action (PDA) ID	Data Actions	Problematic Data Actions and Example Privacy Events	How the Example Solution Architecture Helps Mitigate the PDA	Additional Privacy Mitigations for Organizations to Consider	The Technology Function that Helps Mitigate the PDA
PDA-3: Exposure of patient information through multiple providers of system components	Data about individuals and their devices flows between various applications and analytical tools, some of which are managed by third parties.	Unanticipated Revelation: Multiple organizations work together to provide individual components of the RPM solution and each organization that plays a role in data processing represents an exposure point for patient information.	Combine biometric data with patient identifiers only when operationally required. Protect data transmitted between parties and in storage.	Limit or disable access to data. Use contracts to limit third-party data processing.	Technology Solution 5 Technology Solution 6

NIST Privacy Framework



Privacy Framework Mapped to Solution Capabilities

Problematic Data Actions (PRAM) → Privacy Capabilities/ NIST Privacy Framework Subcategories → Privacy Controls

Privacy Framework Mapping from Draft 1800-30

Table 3-6 Privacy Characteristics and Controls Mapping—NIST Privacy Framework

NIST Privacy Framework v1.0			
Function	**Category**	**Subcategory**	**NIST SP 800-53, Rev 5**
Identify - P	Inventory and Mapping (ID.IM-P)	ID.IM-P1: Systems/products/services that process data are inventoried.	Controls X
		ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.	Controls X
		ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	Controls X
	Risk Assessment (ID.RA-P)	ID.RA-P3: Potential problematic data actions and associated problems are identified.	Controls X
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	Controls X
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.	Controls X
Control – P	Data Processing Management (CT.DM-P)	CT.DM-P5: Data are destroyed according to policy.	Controls X
		CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.	Controls X

Next Steps & Stay Engaged

- **Draft Practice Guide (SP 1800-30) for public comment**
  - Public comment period open through December 18, 2020

- **Securing Telehealth Remote Patient Monitoring Ecosystem**
  - https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth

- **Community of Interest**
  - hit_nccoe@nist.gov

Connect with us

Nakia Grayson

IT Security Specialist

NCCoE& PEP/NIST

nakia.grayson@nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

https://www.nccoe.nist.gov/

@NISTCyber
#NCCoE

Privacy Resources

- **Privacy Framework Website**
  - https://www.nist.gov/privacyframework
- **Privacy Risk Assessment Methodology (PRAM)**
  - https://www.nist.gov/privacy-framework/nist-pra
- **Privacy Framework Mailing List**
  - https://www.nist.gov/privacyframework
- **Privacy Framework Contact Information**
  - PrivacyFramework@nist.gov
  - @NISTcyber #PrivacyFramework

CSG 2020 National Conference REIMAGINED

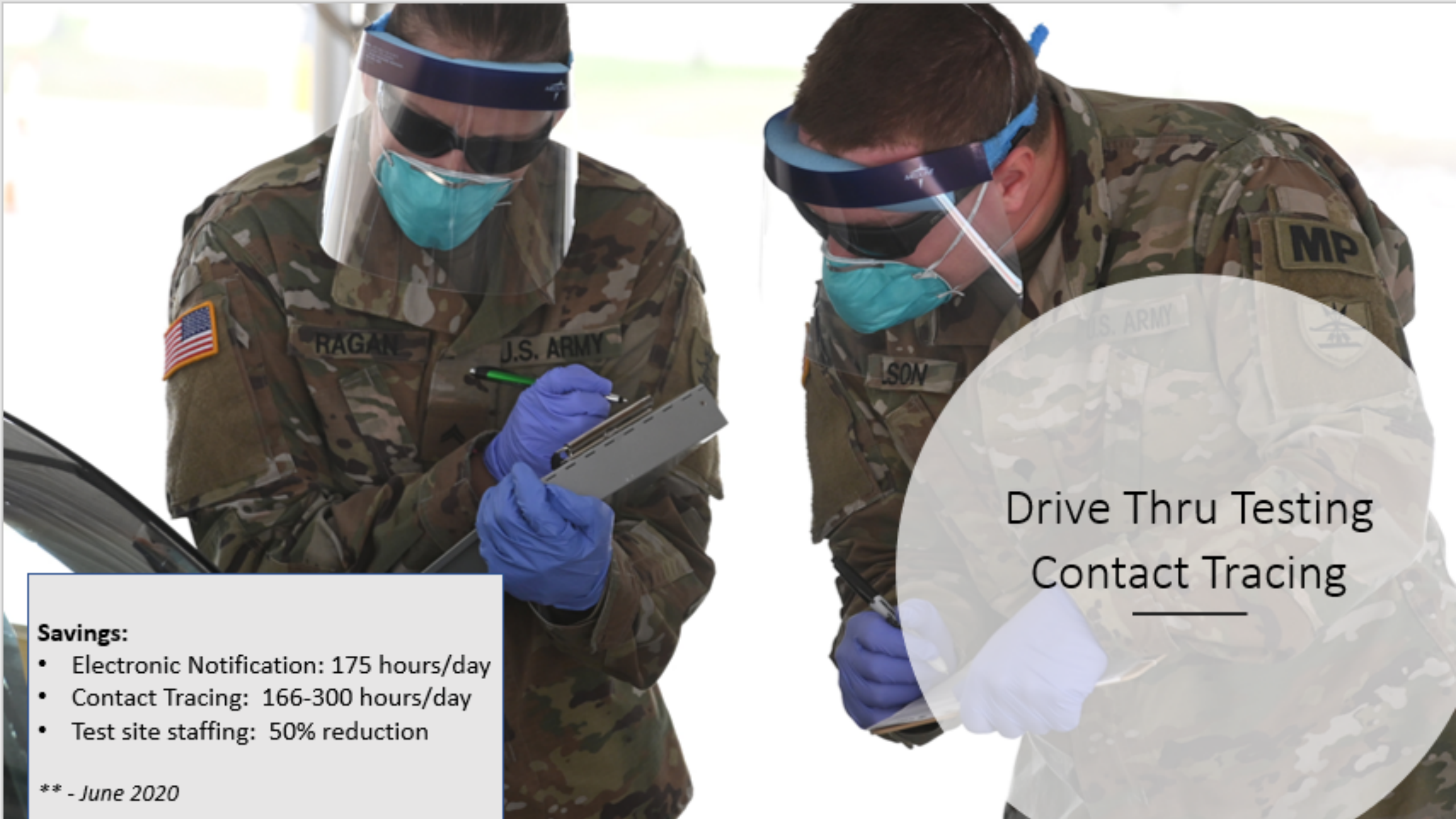
OCT. 26-DEC. 18

NORTH Dakota | Information Technology

Be Legendary.™

COVID – 19 Contact Tracing and Applications

Duane Schell
CTO – State of North Dakota



Drive Thru Testing
Contact Tracing

Savings:

- Electronic Notification: 175 hours/day
- Contact Tracing: 166-300 hours/day
- Test site staffing: 50% reduction

*** - June 2020*

Care19 Diary

The Care19 app that launched in April, by Gov. Doug Burgum and the North Dakota Department of Health (NDDoH) in partnership with ProudCrowd, creators of the popular Bison Tracker app, is NOW Care19 Diary. This application is an easy way for you to record your activity which will be important should you or a close companion test positive.

Individuals will be given a random ID number and the app will anonymously cache the individual's locations throughout the day. Individuals are then encouraged to categorize their movement into different groups such as work or grocery. The app will only store the location of any place a person visits for 10 minutes or more, and the ID number of each individual contains no personal information besides location data.

If an individual tests positive for COVID-19, they will be given the opportunity to consent to provide their information to the NDDoH to help in contact tracing and forecasting the pandemic's progression with accurate, real-time data.

Care19 Alert

Care19 Alert app uses the Bluetooth proximity technology provided jointly by Apple and Google Exposure Notification Systems to keep track of the anonymous keys (transmitted by phones near you) that a user encounters over time.

Care19 Alert quickly notifies you if you've likely been exposed to COVID-19 - empowering you to make decisions that are best for you and your loved ones: like seeking medical advice or staying home. When lots of people use the app it can help public health systems manage the disease and save lives by flattening the curve.

Care19 Alert is the first exposure notification app to connect with the National Key Server provided by the Association of Public Health Laboratories (APHL). Use of this server allows different states' apps to communicate with each other, protecting North Dakotans when they are traveling across state borders or when others are visiting North Dakota and subsequently become COVID-19 positive.

Care19
Alert

CSG 2020 National Conference REIMAGINED

OCT. 26-DEC. 18

HEALTH CARE INFORMATION AND YOUR PRIVACY BILL

December 7, 2020

HEALTH CARE INFORMATION

Lot of information to think about. All of it is regulated by someone – or will be soon. Carving out HIPPO… HYPO? HIPPA? … is not really enough.

HIPAA – Health Insurance Portability and Accountability Act

- Protected Health Information
- Deidentified Health Information
- Covered Entities
- Business Associates

Medical Research – this is extremely complicated

- Common Rule
- International Council for Harmonization

HIPAA PRIVACY RULE & PHI

HIPAA Privacy, Security, Enforcement, and Breach Notification Rules
(Cybersecurity and breach are also covered already)

"Protected health information includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage. 'Protected' means the information is protected under the HIPAA Privacy Rule."

Protected Health Information is complicated and works pretty well.

WHERE THESE RULES COME FROM

National Committee for Vital and Health Statistics

The NCVHS serves as the statutory [42 U.S.C. 242k(k)] public advisory body to the Secretary of Health and Human Services (HHS) for health data, statistics, privacy, and national health information policy and the Health Insurance Portability and Accountability Act (HIPAA). The Committee advises the HHS Secretary, reports regularly to Congress on HIPAA implementation, and serves as a forum for interaction between HHS and interested private sector groups on a range of health data issues.

Subcommittee on Privacy, Confidentiality and Security

HEALTH CARE INFORMATION POLICE

Federal Regulators

- HHS - US Office of Civil Rights does enforce
- Enforcement can be onerous and scary
- FTC can also
- Sometimes FDA gets involved – special circumstances

HIPAA – HITECH Act Amendments of 2009 confer enforcement powers to states attorney generals! Hurray!

Medical research is regulated by FDA. Also by state departments of public health, public universities and institutional review boards (IRBs) – very scary regulator, can shut down research.

HEALTH CARE ENTITIES TO TALK TO

To avoid a stampede of lobbyists into your office and frustrated calls from Governor's Office – do this:

Have your staff or bill supporters reach out to the health care industry and ask for language.

- Doctors: state medical society
- Hospitals: state hospital association
- Clinics
- Mental health treatment groups
- Health plans
- Biotech groups: PhRMA, AdvaMed, BIO, state groups

PLEASE JUST DON'T…

"Property rights" just don't work. Will break health care

Other Issues – FR, AI, biometric, direct-to-consumer, etc
FDA is working on it

Blockchain mandates

"Fix" HIPAA – it is constantly improving. States should stay out

Don't regulate "above" HIPAA standards. Yes you can, but that doesn't mean you should.

Overly complex digital contact tracing regulation bills

THANK YOU!

AdvaMed
Advanced Medical Technology Association

CSG 2020 National Conference REIMAGINED

OCT. 26-DEC. 18

IDAC

International Digital Accountability Council

COVID-19 Mobile App Accountability Project

The Center of Innovation, Council of State Governments

December 7, 2020

About Us

Incubated at the Future of Privacy Forum and launched in April 2020, the International Digital Accountability Council (IDAC) is an independent watchdog with a mission to improve global digital accountability through monitoring, investigation, and education

IDAC

International Digital Accountability Council

COVID-19 App Study

On June 5, we released a report on COVID-19 apps. We examined the privacy implications behind these apps with the goal of identifying issues and offering actionable recommendations to instill public trust.

Our study included:

- 108 COVID-19 Android mobile apps (as of May 1, 2020)
- Spanning 41 countries
- Categories: Symptom Checkers, Contact Tracing, Quarantine Administration, and Telehealthcare

IDAC
International Digital Accountability Council

COVID-19 Report Key Findings

Although we did not find egregious or willful misconduct, the rushed nature under which these apps were created has led to developers using tools and approaches that are (in some cases) ill-advised for the sensitivity of COVID-19 data.

1 - Transparency

2 - SDKs

3 - Security

4 - Permissions

IDAC
International Digital Accountability Council

Technical Methodology

We ran static and dynamic tests on the apps, as well as how the apps operated in real-time. Next, we ran our analysis on the network traffic and operating system information.

Tests revealed:

- Types of personal data apps collect
- Who the data is being sent to
- Types of permissions requested
- Types of software development kits (SDKs) present in the app

IDAC
International Digital Accountability Council

Finding #1 – Transparency

Not transparent about their data collection and third-party sharing practices.

- ✖ Third parties not disclosed on privacy policies
- ✖ Vague or inexistent privacy policies

IDAC
International Digital Accountability Council

Finding #2 - SDKs

Presence of third-party software development kits (SDKs), which could lead to external data sharing without users' knowledge.

- ✖ Analytics and Advertising SDKs
- ✎ Developers should be more careful with what information SDKs might be collecting, and understanding the implications of this collection

IDAC
International Digital Accountability Council

Finding #3 - Security

Apps sent unencrypted transmissions, as well some API endpoints open to the public that transmitted location and symptom reports of other users.

! All transmissions should be done over HTTPS

IDAC
International Digital Accountability Council

Finding #4 - Permissions

Apps requested permissions that have the potential to be invasive and exceeded the information that is reasonably necessary to provide its services.

“Read external storage” or “write external storage” allows the app to access shared files on the phone that could be used to infer personal information.

IDAC
International Digital Accountability Council

IDAC Recommendations

Transparency

- ✓ Disclose collection, data sharing, and retention practices
- ✗ Copy from other privacy policies or be vague

SDKs

- ✓ Only include necessary SDKs
- ! Review third-party SDKs and understand their data collection and sharing practices

Security

- ✓ Always send data using HTTPS or TLS protocol

Permissions

- ✓ Only request what is needed for app's core functions

IDAC
International Digital Accountability Council

COVID-19 Report Immediate Impact

IDAC has worked with developers to address concerns raised in the report. Outcomes:

- Implementing privacy policies
- Retiring unnecessary SDKs
- Stopping inappropriate third-party data sharing

IDAC
International Digital Accountability Council

COVID-19 Report Next Steps

IDAC's report has been covered by international media outlets, educating the public on the risks of COVID-19 apps.

IDAC has continued its work in the COVID-19 digital space by:

- Educating governments, state leaders, and other stakeholders
- Monitoring the evolving COVID-19 digital space
- Offering recommendations on COVID-19 US legislation

IDAC
International Digital Accountability Council

Looking Ahead

Beyond its COVID-19 work, IDAC plans to continue working on:

- Accountability
- Developer education
- Norm development

IDAC
International Digital Accountability Council

IDAC

International Digital Accountability Council

THANK YOU

QUENTIN PALFREY | President of IDAC

(617) 290-8348

qpalfrey@digitalwatchdog.org

CSG

CSG 2020 OCT. 26-DEC. 18

National Conference

REIMAGINED

Hon. Frank LaRose

Secretary of State, Ohio

CSG

CSG 2020 National Conference REIMAGINED

OCT. 26-DEC. 18

Michael Leahy
Secretary of Information Technology, Maryland

Michael Hussey
Chief Information Officer, Utah

Dylan Gilbert
Privacy Policy Advisor, National Institute of Standards and Technology

NIST Privacy Framework: a Tool for Improving Privacy through Enterprise Risk Management

Version 1.0

December, 2020

National Institute of Standards and Technology
U.S. Department of Commerce

Value Proposition

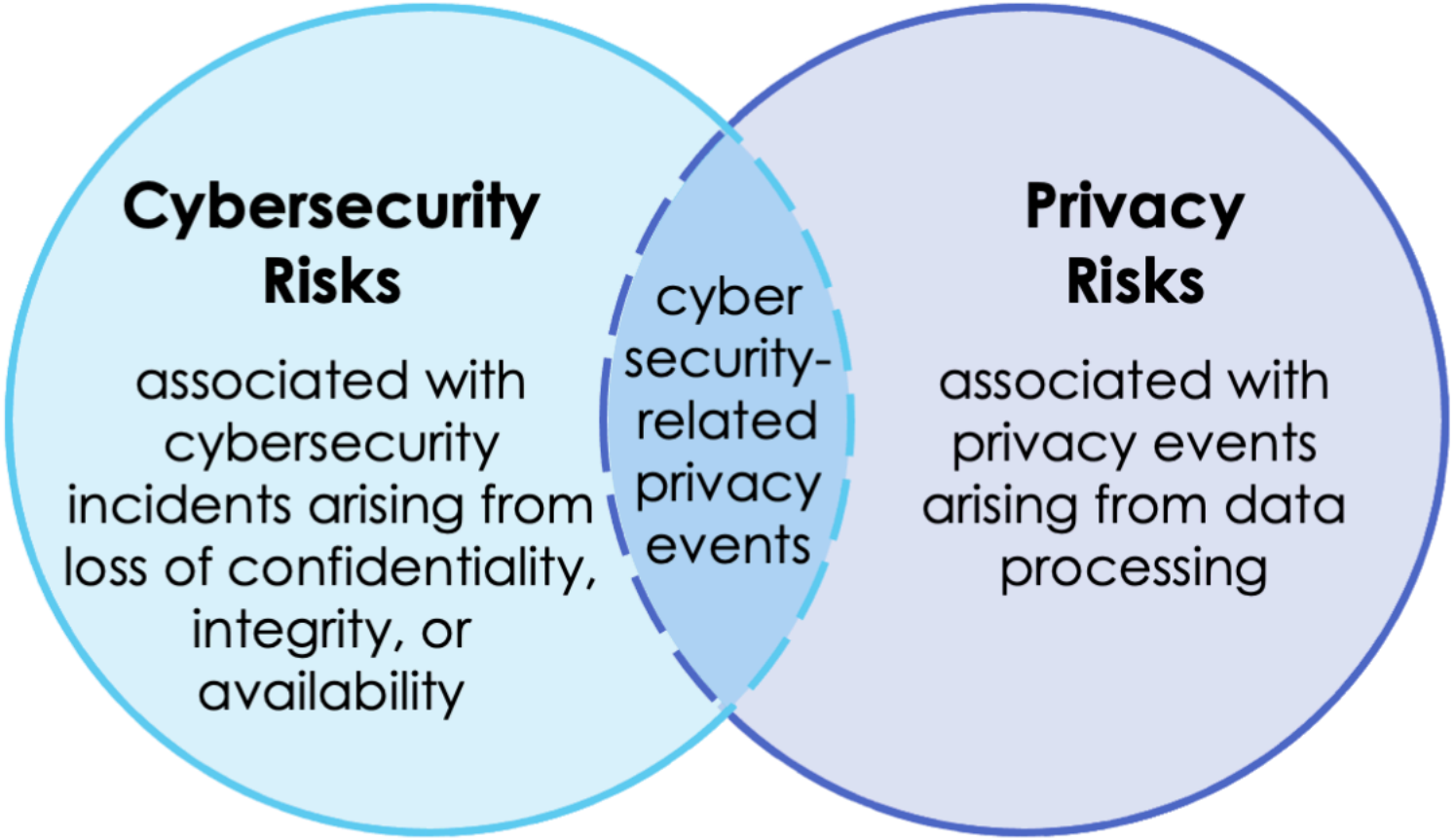
Privacy Framework supports:

Building customer trust

Fulfilling current compliance obligations

Facilitating communication

Relationship Between Cybersecurity and Privacy Risk



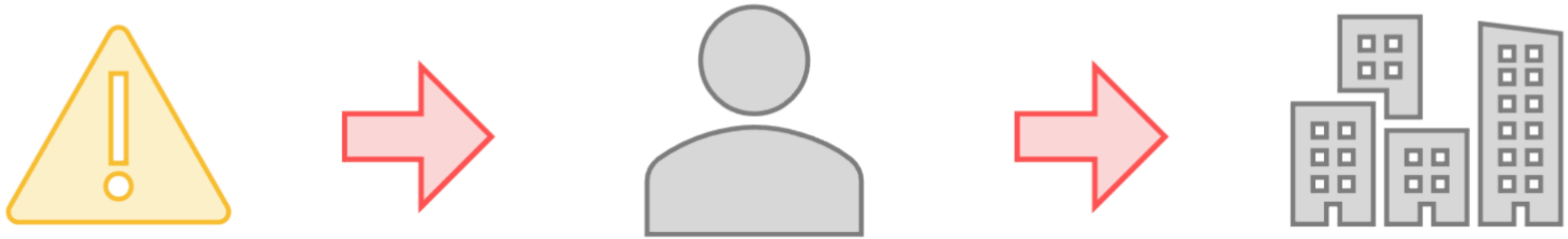
Data: A representation of information, including digital and non-digital formats

Privacy Event: The occurrence or potential occurrence of problematic data actions

Data Processing: The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal)

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

Privacy Risk and Organizational Risk



Problem

arises from data processing

Individual

experiences direct impact
(e.g., embarrassment, discrimination, economic loss)

Organization

resulting impact
(e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

FRAMEWORK STRUCTURE

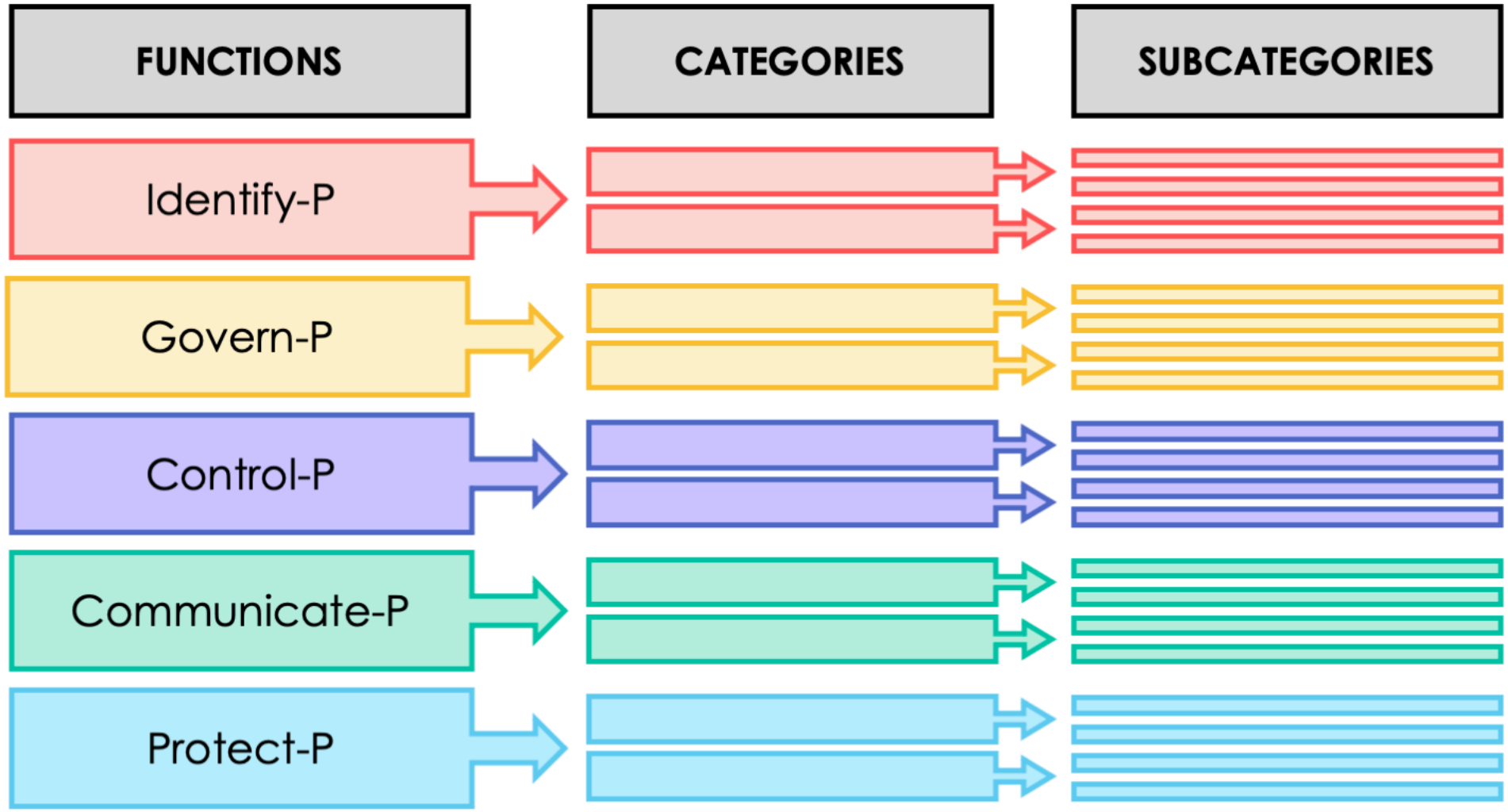
Privacy Framework Structure

The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that the organization has prioritized to help it manage privacy risk

Implementation Tiers help an organization communicate about whether it has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile

Privacy Framework Core



Example Subcategories

ID-P	ID.IM-P	**ID.IM-P8**	Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.
GV-P	GV.PO-P	**GV.PO-P5**	Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
CT-P	CT.DP-P	**CT.DM-P1**	Data elements can be accessed for review.
CM-P	CM.AW-P	**CM.AW-P1**	Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
PR-P	PR.AC-P	**PR.DS-P1**	Data-at-rest are protected.

How to Use the Privacy Framework

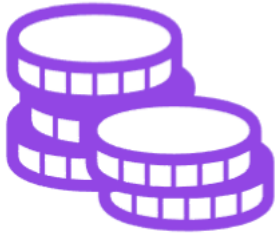
Informative References

Strengthening Accountability

Establishing or Improving a Privacy Program

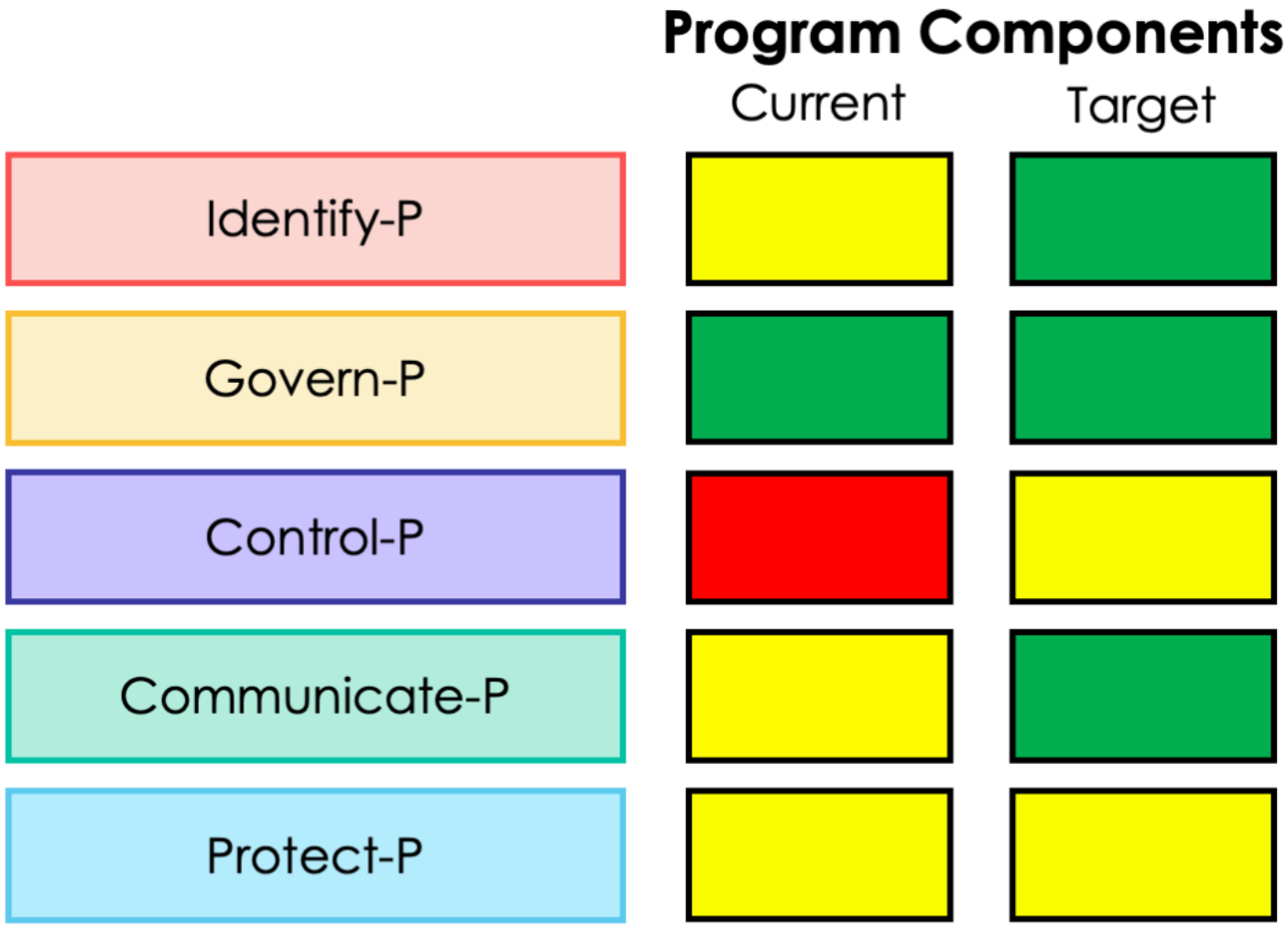
Applying to the System Development Life Cycle

Using within the Data Processing Ecosystem

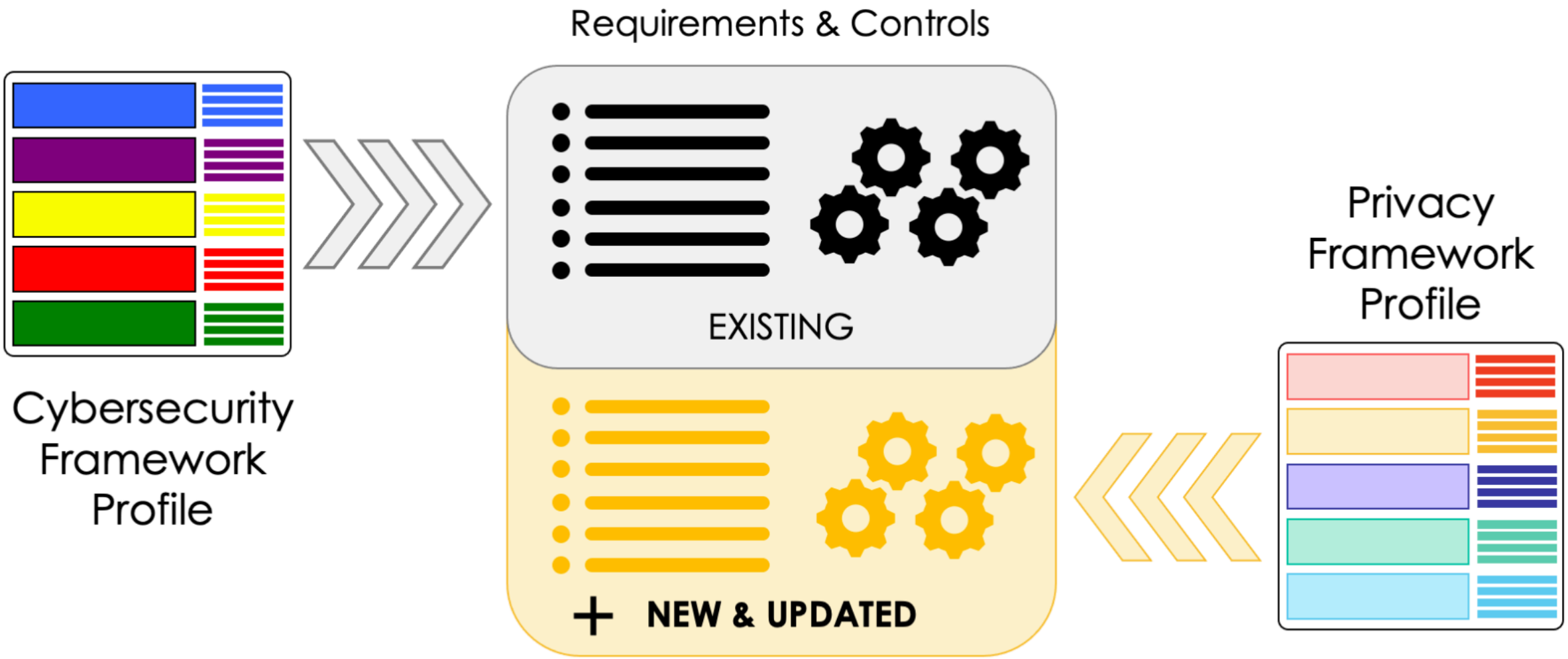


Informing Buying Decisions

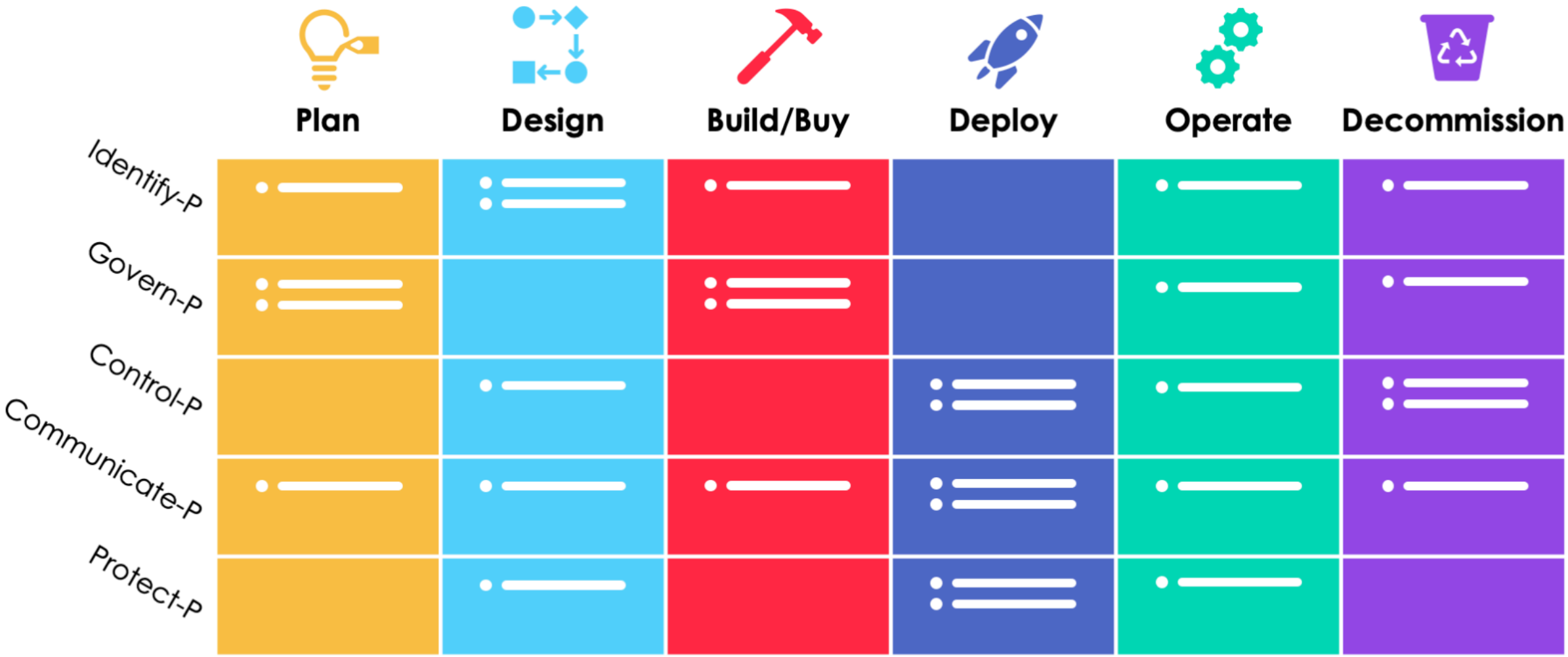
Communication and Advocacy with Leadership Example



Program Alignment Example



System Development Life Cycle Example



NEXT STEPS

Adopt me!

- Lead on privacy
- Provide implementation feedback
- Contribute resources to the NIST's Resource Repository

Resources

Website

https://www.nist.gov/privacyframework

Mailing List

https://groups.google.com/a/list.nist.gov/forum/#!forum/privacyframework

Contact Us

PrivacyFramework@nist.gov

@NISTcyber #PrivacyFramework

CSG

CSG 2020 OCT. 26-DEC. 18
National Conference
REIMAGINED

At the conclusion of today's session, please remember to take the policy academy survey available at the link in the Chat:

https://www.surveymonkey.com/r/C29VX57

CSG

CSG 2020 OCT. 26-DEC. 18
National Conference
REIMAGINED

Don't Miss These Upcoming Sessions

Shared State Legislative Committee
Dec. 8 & 9 | 2 - 5 p.m. ET

An Interstate Compact for Teacher License Mobility
Dec. 10 | 2 - 3 p.m. ET

Sustainability in the COVID Era Policy Academy
Dec. 11 | 1 - 5 p.m. ET

View the full list of sessions at *web.csg.org/2020*