# NIST Cyber Risk Scoring (CRS)

### **Program Overview**

February 2021



### Agenda



- CRS Project Background
- Risk Profiling and Risk Scoring
- Information Security Continuous Monitoring (ISCM) & Ongoing Authorization (OA)
- Privacy Capabilities
- Management Dashboards
- Questions?

### Assessing, Understanding, and Managing Security and Privacy Risks



NIST's Cyber Risk Scoring (CRS) Solution enhances NIST's security & privacy Assessment & Authorization (A&A) processes by presenting real-time, contextualized risk data to improve situational awareness and prioritize required actions.

**Previous Process** 







# Benefits of CRS



- Integrated view of NIST risk posture across the enterprise with quantitative metrics across systems and components
- More frequent, meaningful and actionable risk information to System Owners & Authorizing Officials
- Improved efficiency through automating assessments of certain controls and auto-generation of ATO documentation
- A data-driven basis for ongoing authorization decisions
- Present the organization's overall security posture from different perspectives, e.g., the Risk Management Framework (RMF) and Cyber Security Framework (CSF)

## **CRS** Capabilities



The CRS toolset provides end users the following capabilities:

### Archer:

- Prioritize security & privacy control assessments
- Manage A&A and significant change schedules
- Track Accepted Risks and POA&M milestones
- Generate security and privacy documentation
- Provide compliance and vulnerabilities scan results in near-real time

### Tableau:

- View risk at multiple organizational levels
- Integrate vulnerability data into risk scoring
- Drill-down into specific assets and their current vulnerability exposures
- Respond to data calls quickly with details (e.g. CVEs and affected assets)
- Analyze risks against the CSF

### **CRS** Inputs



These data are ingested into Archer and analyzed for presentation in Tableau.



### **CRS** Outputs



After analysis users can generate ATO documentation on-demand & view metric-based risk management dashboards.



### **Risk Profiling and Scoring**

# **Risk Profiling Overview**



- Risk Profiling is a process that allows NIST to determine the importance of a system to the organization's mission.
- By first understanding the **business and technical characteristics** that impact system risk, an agency can **identify and align controls to a component** based on the likelihood that a weakness will be exploited and the **potential impact to the organization**.

1. Define Organization's Risk Factors and Priorities	2. Develop Business and Technical Characteristics		3. Determine Tailoring Logic & Apply Common Controls		4. Incorporate Compliance and Vulnerability Data		5. Deploy Continuous Monitoring
Organization's priorities and <b>risk</b> <b>appetite is</b> <b>determined</b> by receiving input <b>from</b> <b>stakeholders</b> to customize a security questionnaire that will best fit the organization's security needs.	Questionnaire is created to reflect organization's business processes and technical environment. Likelihood and threat factors tied to these characteristics are quantified.	•	The Risk Profile leverages Common Control Providers and scoping considerations to reduce the number of controls to be assessed, narrowing the scope of work while maintaining security awareness.	•	Assessment, compliance, and vulnerability data is continuously recorded in the Risk Profile to determine the risk posture of the information system.	•	The Risk Profile makes it possible to perform Continuous Monitoring of all implemented security and privacy controls by using a <b>risk-based</b> <b>approach to</b> <b>prioritize control</b> <b>assessments.</b>
Output: Risk Profile Methodology	Output: Risk Profile Multiplier		Output: Applicable Controls and Total Potential Risk		Output: Total View of Risk		Output: Metric Reports

## **Risk Scoring Variables**



Risk Scoring provides a foundation for **quantitative risk-based analysis**, assessment, and reporting of organizational IT assets. By applying ratings to controls and generating scores for components, stakeholders have a **relative understanding of risk** from one system compared to another.

The variables that can affect a control's potential risk score is outlined below.

Variable	Description	Considerations
Control Baseline Risk Score	Every control is assigned an initial weighting (1-10) based on an analysis of its importance to the security and privacy posture.	<ul> <li>What is the potential security impact of this control to NIST?</li> </ul>
Data Type Questionnaire Responses	Initial CIA ratings (1-10) are assigned to controls, based on criticality of the information type(s), upon completion of the Data Type Questionnaire.	<ul> <li>What is the impact of Confidentiality (C), Integrity (I), and Availability (A) to the types of information that are used within this component?</li> </ul>
Risk Profile Questionnaire Responses	Additional adjustments are applied as indicated by responses to the Risk Profile Questionnaire, including business risks.	<ul> <li>What assets or applications are part of the component?</li> <li>What is potential security impact of this component to the enterprise?</li> </ul>

# **Risk Calculation Overview**



The following steps are completed in Archer for each system component to calculate potential risk.

### **Complete Questionnaires**

l	?
l	?

- Data Type Questionnaire:
   Determines an overall system security category for the component, assigns the security control "baseline" (Low/Moderate/High), and calculates initial risk score modifier.
- Risk Profile Questionnaire: Performs additional control scoping and calculates final risk score modifiers for the resulting set of applicable controls.

**Generate Risk Profile** 



- The Risk Profile outlines the **controls** that should be implemented.
- Security controls are assigned ratings for Confidentiality, Integrity, and Availability to quantify risks.
- Components are assessed based on their implementation of these controls.

### **Calculate Risk Score**





- The sum of all Component potential risk equals the System potential risk
- Final scores include a **multitude of security inputs** (e.g., manual inputs, vulnerabilities, compliance scans).
- Risk scores create the ability to make "apples-to-apples" comparisons across the enterprise.

### Information Security Continuous Monitoring and Ongoing Authorization Approach



ISCM promotes more frequent and targeted monitoring of system security and privacy posture to enable risk-based Ongoing Authorization (OA) decisions.

Through CRS, NIST implements ISCM and OA by:

- Prioritizing the set of controls to be evaluated for each assessment
- Providing on-demand reporting of security and privacy metrics (SARs, SAPs, PAPs, and PARs) and management dashboard summaries

## NIST System ATO Schedule



- NIST has 46 operational systems + Common Controls
- NIST System ATOs are on a semi-annual ATO Cycle
- ATO status is managed in Cyber Risk Scoring solution (Archer)



# **ISCM Schedule for Security Controls**

NIST

Security control assessments are prioritized based on importance to the organization (DoC Volatile Controls and Common Controls) and number of potential risk points.

### Sample Assessment Schedule

	Auto	omated		Asse	essment Typ	e		Scan Frequency						
	Asse	essments		Vulnerabilities				Weekly						
				Compliance Scans					Monthly					
				Web Applications			Annual	ly and as ne	eded					
	Mar	nual Assessments*		Controls	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6				
				DoC Volatile Controls										
		Full control set assessed annually		Common Controls										
		Half of the control set is assessed each year		High Risk Controls*										
		One third of the control se assessed each year	et is	Moderate Risk Controls*										
		One sixth of the control se assessed each year	et is	Low Risk Controls*										

\*Risk score ranges were determined by calculating baseline risk score multipliers

## **Assessment Process**

### System Level Data



### Archer captures system information that supports ongoing assessment and authorization efforts.

General	ST&E Activities	High Level Findings	POA&Ms	Accepted Risks	System Artifacts	PTA/PIA	SAP	PAP	ISCM FY2021	ISCM FY2020	
GENERAL INFO	RMATION										
	* System ID:	ļ.					* CSAM	ID: 2252			
	* 0,000	Updated by on 11/16/2015 10	):41:53 AM								
	* System Name:					Last Aut	thorization Da	te: 10/30/202	0		
		Updated by Enloe, Christian o	on 3/26/2020 12:54:0	06 PM							
	Division:	100 Director's Office			<b>S</b>	AIO	Expiration Da	te: 10/30/2021	I		
	Compliant:					PIA SAOP A	Authorized Da	te:			
System Ope	rational Status (CSAM):	Operational			•	WebInspec	t VSA Start Da	te:		<b></b>	
	System Description:	The NIST Director's Office (D	O) System supports	the day-to-day functions	of the NIST DO suite, NIST	Office of General	Counsel, Execu	tive Officer for	Administration and all	related divisions/office	s, Chief of Staff and all related
		divisions/onices, and the third		rs (AD) top level offices.							
		The Divisions covered within	the scope of this sy	stem are as follows:							
		Division Number	Staff Office Name Director's Office: O	ffice of the Chief Couns	sel: Executive Officer						
		100	for Administration;	Office of the Chief of St	taff; Onboarding Office						$\sim$
Syste	m Migrated To Archer?:	Yes	Management and C		1		Contains P	II?: No			
Overall Sys	stem Security Category:	Moderate					Contains B	II?: No			
	Overall Confidentiality:	Moderate									
	Overall Integrity:	Moderate									
	Overall Availability:	Low									

### Tailored Control Set



Upon completion of the questionnaires, each component is provided with a tailored set of controls.

Component :							8			
EDIT VIE	W SAVE SAVE	E AND CLOSE								
First Published: 6/1/2017 3:4	19 PM Last Updated: 9/24/2020	11:04 AM				0 B ±	⊻	Tailorod Controls :	AC 2	$\otimes$
General Inte	erconnections Data	a Type Questionnaire	Risk Profile Questionnai	re Security Tail	ored Controls	Privacy Tailored Controls	^			-
Security Assessment F	Results Privacy Ass	essment Results A	ssets Risk Summa	ary ISCM FY2020			_	First Published: 6/2/2017 10:19 PM Last LL	ndated: 8/20/2019 9:43 AM	<b>A + M</b>
► CONTROL SUMMARY	1							General Risk Scores	CCP Implementation Statement	
▼ TAILORED CONTROL	S					Add New   Loo	kup		cer implementation statement	
Control Family	Control Number	Control Name	Baseline	Control Applicability	Assessment Date	Control Status		Potential 284	Potential 284	
Access Control	<u>AC-1</u>	Access Control Policy and Procedures	Low Moderate High	Hybrid	7/26/2019		8	Risk - (SOR): Mitigated 284 Risk - (SOR):	Risk: Mitigated 284 Risk:	
Access Control	<u>AC-2</u>	Account Management	Low Moderate High	Applicable	7/19/2019	Satisfied	8	Kesidual 0 Risk - (SOR): Residual 0 Risk - Accept Risk (SOR):	Residual () Risk: Residual () Risk - Accept Risk:	
Access Control	<u>AC-2(1)</u>	Automated System Account Management	Moderate High	Applicable	7/19/2019	Satisfied	8	Residual 0 Risk - POA&M	Residual 0 Risk - POA&M:	
Access Control	<u>AC-2(2)</u>	Removal of Temporary/Emergency Accounts	Moderate High	Applicable	7/26/2019	Satisfied	8	(SOR):		
Access Control	<u>AC-2(3)</u>	Disable Inactive Accounts	Moderate High	Applicable	7/19/2019	Satisfied	8			
Access Control	<u>AC-2(4)</u>	Automated Audit Actions	Moderate High	Applicable	7/19/2019	Satisfied	8			

### **Control Assessment Input**



Assessors can document assessment results and supporting details in this interactive form.



## SAP/SAR Generation



The images below show the Security Assessment Plan (SAP) and Security Assessment Report (SAR) Assessors complete in Archer. Upon completion of assessments, the documentation is generated directly from Archer.

### **Security Assessment Plan**

	216 11:43 AM Last I	Updated: 8/17/2020 9:29 AM										0 ± 1	
	ST&E Activities	High Level Findings	POA&Ms	Accepted Ris	iks System Artifai	cis PTA/PIA	SAP	PAP ISCM PY2020					
Disple	ey Report" below	to view the Security SAP for	this system.										
	NISCM EV & TRD	" It has not have specified a	han the control peaks to be a	errarrad The	ISCH EV for an entermant of	f that countrol will be d	atermined at the and	of the current fireal user.					
									D2				
REPO	ORT					14	4 1 to 250 (of 4.356)	> >i				C REF	FRESH
6	Component	Control Number	Cantrol Name	Assessment	ISCM FY	Control Applicability	Control Applicability	Brason for Overrain	Control Inherited	from Control Status	New Assessment	Assessment Meth	had
		40.1	Access Control Bolicy and	Date 7/26/2010	2024	Hidered	Overrade		CCP Div 181 (DIS	MIT Sec	heputt	Examine	
			Procedures			1000			urity Policies)				
		10.1	Annual Control Dates and	8/10/2010	2024		No. A. of		(CR Du 181 (OF	All face Frencher	Freiderd	Provide a	
		0.0	Procedures	0/13/2019	2004	riyuran .	nyunu		urity Policies)	will ber Saturned	Securied	Exemine	
													_
1	Auto	oSave 💿 off) 🖳	<b>P1 19 ·</b> (2 ·		150-0	01 SAP.xlsx - Sa	wed	Table Tools		Cascio, John J	(Ctr)	<b>=</b> –	
1	ion		- / \								· · •		
					provular Data	Poviow	View H	elp Design 🖓	Search			🖻 Share	P
	File	Home Ins	ert Page Layou	JT FC	ormulas Dala	i Neview	view ii						
	File I10	Home Ins	ert Page Layou	JT FC	omulas Dala	i Keview							
	File I10	Home Ins	ert Page Layou	ut FC	omulas Dala	. Keview		,					
	File	Home Ins	ert Page Layou	ut Fo	D	E		F G		н		I	
	File	A B A Compone	c Control Nur	nber 🔽	D Control Name	E Assessmen	t Date VISCI	F G M FY Control Applicabi	ility <b>Z</b> Control Appl	H icability Overrid	e 💌 Reason f	l or Override	• Co
	File	A B Home Ins A B Iex Compone	c AC-1	nber 🔽	D Control Name Access Control I	E Assessmen Pc 7,	t Date v ISCI /26/2019	F G M FY Control Applicabi 2024 Hybrid 2024 Hybrid	líty <mark>–</mark> Control App Hybrid Hybrid	H icability Overrid	e 🔽 Reason f HAPPY h	I or Override s as additional	▼ Co arCC
	File 110 1 Ind 2 3	A B A B Iex Component	c C C C C C C C C C C C C C	nber 💌	D Control Name Access Control I Access Control I	E Assessmen Pc 7, Pc 8, 8,	t Date V ISCI /26/2019 /13/2019	F G VI FY Control Applicabi 2024 Hybrid 2024 Hybrid 2025 Applicable	l <mark>ility ▼</mark> Control Appl Hybrid Hybrid	H icability Overrid	e 💌 Reason f HAPPY h HU has a	l or Override as additional dditional acce	✓ Co arCo es Co
	File 110 1 Ind 2 3 4	A B A Component 1 1 1	ert Page Layor	nber 💌	D Control Name Access Control I Access Control I Access Control I	E Assessmen Pc 7, Pc 8, Pc	t Date V ISCI /26/2019 /13/2019 /15/2018 vocume	F G M FY Control Applicabi 2024 Hybrid 2025 Applicable 2025 Lobected	ility <mark>– Control App</mark> Hybrid Hybrid	H icability Overrid	e 🔽 Reason fi HAPPY hi HU has a	l or Override as additional dditional acce	▼ Co ai CO es CO
	File 110 1 Ind 2 2 3 4 4 5 5 6	Home Ins	rt Page Layor	nber 🗸	D Control Name D Access Control I Access Control I Access Control I Access Control I	E Assessmen Pc 7, Pc 8, Policy and Pro	t Date ▼ ISCI /26/2019 /13/2019 /15/2018 ocedures	F G M FY Control Applicabi 2024 Hybrid 2025 Applicable 2025 Inherited 2025 Inherited	ility <mark>z Control App</mark> Hybrid Hybrid	H icability Overrid	e Reason f HAPPY h HU has a	l or Override as additional dditional acce	✓ Co ai CO es CO
	File 110 1 Ind 2 3 4 5 6 6	A B Ex Compone 1 1 1 1	ert Page Layor × ✓ ♪ C C AC-1 AC-1 AC-1 AC-1 AC-1 AC-1 AC-1 AC-1 AC-1	nber 🗸	D Control Name S Access Control I Access Control I Access Control I Access Control I Access Control I	E Assessmen Pc 7, Pc 8, Policy and Pro Policy and Pro	t Date V ISCI /26/2019 /13/2019 /15/2018 scedures scedures	F G M FY' Control Applicable 2024 Hybrid 2024 Hybrid 2025 Applicable 2025 Inherited 2026 Inherited	ility <mark>☞</mark> Control Appl Hybrid Hybrid	H icability Overrid	e Reason f HAPPY h HU has a	l or Override as additional dditional acce	<ul> <li>Co ai CO es CO CO CO CO CO CO CO</li> </ul>
	File 110 1 Ind 2 3 4 5 6 6 7 2	Home Ins	ert Page Layor × ✓ fr C C AC-1 AC-1 AC-1 AC-1 AC-1 AC-1 AC-1 AC-1 AC-1 AC-1	nber 💌	D Control Name S Access Control I Access Control I Access Control I Access Control I Access Control I Access Control I	E Assessmen Pc 7, Pc 8, Policy and Pro Policy and Pro Policy and Pro	t Date V ISCI /26/2019 /13/2019 /15/2018 ocedures ocedures ocedures	F G M FY Control Applicabl 2024 Hybrid 2025 Applicable 2025 Inherited 2026 Inherited 2024 Inherited 2024 Inherited	lity V Control App Hybrid Hybrid	H icability Overrid	e <b>Reason f</b> HAPPY hi HU has a	l or Override as additional dditional acce	<ul> <li>CC</li> <li>a) CC</li> <li>es CC</li> <li>CC</li> <li>CC</li> <li>CC</li> <li>CC</li> </ul>
	File 110 1 Ind 2 Ind 2 Ind 3 Ind 3 Ind 5 Ind 6 Ind 7 Ind 8 Ind 9 Ind	A B Ex Compone	rt Page Layor × ✓ fr C cntrol Nur AC-1	nber 🔽	D Control Name S Access Control I Access Control I Access Control I Access Control I Access Control I Access Control I Access Control I	E Assessmen Pc 7, Pc 8, Policy and Pro Policy and Pro Policy and Pro Policy and Pro Policy and Pro	t Date v ISCT /26/2019 /13/2019 /15/2018 ocedures ocedures ocedures TBD ocedures TBD	F G MFY Control Applicabi 2024 Hybrid 2024 Hybrid 2025 Applicable 2025 Inherited 2024 Inherited 2024 Inherited 2024 Inherited 2024 Inherited 2024 Inherited	liity Control Appl Hybrid Hybrid	H icability Overrid	e Y Reason f HAPPY h HU has a	I or Override S as additional dditional acce	✓ CC ai CC es CC CC CC CC
	File 110 1 Ind 2 3 4 5 6 7 8 9 9	Home ins	ert Page Layor × ✓ <i>f</i> / Control Num AC-1	nber 🗸	D Control Name Access Control I Access Control I	E Assessmen Pc 7, Pc 8, Policy and Pro Policy and Pro Policy and Pro Policy and Pro Policy and Pro	t Date v ISCT /26/2019 /13/2019 /15/2018 ccedures ccedures ccedures ccedures ccedures	F G M FY Control Applicabl 2024 Hybrid 2025 Applicable 2025 Inherited 2024 Inherited 2024 Inherited 2024 Inherited 2024 Inherited 2025 Inherited 2025 Inherited	liity - Control Appl Hybrid Hybrid	H icability Overrid	e V Reason f HAPPY h HU has a	I or Override as additional acce	▼ Co ai CO es CO CO CO CO CO
	File 110 1 Ind 2 3 4 5 6 7 8 9 10 11	Home Ins	err         Page Layor           X         F           Control Nur         CC-1           AC-1         AC-1	nber -	D Control Name 1 Access Control I Access Control I	EE     EE     Assessmen     Pc     7,     Pc     8,     Policy and Prc     Policy an	t Date V ISCI [26/2019 /13/2019 /10/2019 /10/2019 /10/2019 /10/2019 /10/200	F G M FY Control Applicable 2024 Hybrid 2025 Applicable 2025 Inherited 2024 Inherited 2024 Inherited 2024 Inherited 2024 Inherited 2025 Inherited	lify Control Appl Hybrid Hybrid	H icability Overrid	e 🛛 Reason f HAPPY h HU has a	I or Override as additional acce	<ul> <li>CC</li> <li>a) CC</li> <li>es CC</li> <li>CC</li> <li>CC</li></ul>
	File 110 1 Ind 2 Ind 3 Ind 4 Ind 5 Ind 7 Ind 8 Ind 9 Ind 11 Ind 1	Home Ins	rt Page Layor × ✓ fr Control Num AC-1	nber -	D Control Name Access Control I Access Control I	E Assessmen Pc 7, Pc 8, Policy and Pcc Policy and Pcc Policy and Pcc Policy and Pcc Policy and Pcc Policy and Pcc Policy and Pcc	t Date V ISCI /26/2019 /13/2019 /15/2018 ccedures ccedures ccedures TBD ccedures TBD ccedures TBD ccedures TBD ccedures	F G MEY Control Applicabi 2024 Hybrid 2025 Applicable 2025 Applicable 2025 Inherited 2024 Inherited 2024 Inherited 2025 Inherited Not Applicable 2025 Inherited Not Applicable 2025 Inherited	liity Control Appl Hybrid Hybrid	H icability Overrid	e 🔽 Reason f HAPPY hi HU has ar	I or Override S additional acce	<ul> <li>CC</li> <li>a) CC</li> <li>es CC</li> <li>CC</li> <li>CC</li> <li>CC</li> <li>CC</li> <li>CC</li> </ul>
	File 110 1 Ind 2 3 4 5 6 7 8 9 10 11 12 12 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Home Ins	ett         Page Layor           X         Fr           Control Nur         AC-1           AC-1         AC-1	nber 💌	D Control Name Access Control I Access Control I	E E     Assessmen     Pc     Assessmen     Pc     Assessmen     Pc     B     Pc     B     Policy and Prc     Policy andPrc     Policy andPrc	t Date v ISCT /26/2019 /15/2018 ccedures ccedures ccedures TBD ccedures TBD ccedures ccedures TBD ccedures TBD ccedures	F G MFY'= Control Applicabi 2024 Hybrid 2025 Applicable 2025 Inherited 2024 Inherited 2024 Inherited 2024 Inherited 2025 Inherited 2025 Inherited 2025 Inherited Not Applicable 2025 Inherited	liity Control Appl Hybrid Hybrid	H icability Overrid	e X Reason f HAPPY h HU has a	I or Override as additional acce	▼ CC a+CC cc CC CC CC
	File 110 1 Ind 2 Ind 3 4 4 5 6 7 7 8 9 9 10 1 11 12 13 14	Home Ins	rt Page Layor × ✓ fr Control Control Contro	nber 🗸	D Control Name E Access Control Access Control	E     E     Assessmen     Pr     7     Pc     8     Policy and Prc     Policy and Pr	t Date V ISCI /26/2019 /13/2019 /13/2019 /13/2018 ccedures ccedures ccedures ccedures ccedures ccedures tocedures tocedures tocedures tocedures tocedures	F G MFY Control Applicable 2024 Hybrid 2025 Applicable 2025 Inherited 2024 Inherited 2024 Inherited 2024 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2029 Inherited 2029 Inherited 2029 Inherited 2029 Inherited 2029 Inherited 2029 Inherited 2029 Inherited 2029 Inherited 2029 Inherited 2020 Inherited 202	lity Control Appl Hybrid Hybrid	H icability Overrid	e 💌 Reason f HAPPY h HU has at	I or Override as additional acce	<ul> <li>Co</li> <li>a) Co</li> <li>es Co</li> <li>co</li> </ul>
	File 110 1 Ind 2 3 4 4 5 6 7 7 8 9 10 10 11 12 13 14 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Home Ins	rt Page Layor × ✓ fe Control Num AC-1	mber 💌	D Control Name Access Control I Access C	E E Acsessment Pc 7 Acsessment Pc 8 Policy and Pro- Policy and Pro-	t Date v ISCT /26/2019 /13/2019 /13/2019 /13/2019 /13/2019 /13/2019 /13/2019 /13/2019 /13/2019 /13/2019 /13/2019	F G M FY Control Applicabl 2024 Hybrid 2025 Applicable 2025 Inherited 2024 Inherited 2024 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2025 Inherited	iiity - Control Appl Hybrid Hybrid	H icability Overrid	e V Reason f HAPPY h HU has a	I or Override as additional dditional acce	<ul> <li>Co</li> <li>a) Co</li> <li>co</li> <l< td=""></l<></ul>
	File 10 1 Ind 2 3 4 5 6 7 7 8 9 10 11 12 13 14 15 5	Home Ins	Page Layor           X         fx           Control Num         Cc-1           AC-1         AC-1           AC-2         AC-2	nber v	D Control Name 1 Access Control I Access	E E Assessmen Pc 7, Pc 8, Policy and Pro- Policy and Policy and Pro- Policy and Pro- Policy and Policy and Pro- Policy and Pro- Polic	t Date ▼ ISCI /2/2/2019 /13/2019 /13/2019 /13/2019 /13/2019 cedures cedures cedures TBDD cedures TBD cedures TBDD	F G M FY Control Applicable 2024 Hybrid 2025 Applicable 2025 Applicable 2025 Inherited 2024 Inherited 2024 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2025 Inherited 2020 Hybrid 2020 Hybrid	lifty V Control Appl Hybrid Hybrid	H icability Overrid	e 💌 Reason f HAPPY h HU has ar	I or Override as additional acce	<ul> <li>Co</li> <li>a) Co</li> <li>co</li> <l< td=""></l<></ul>

### System : EDIT VIEW 6 11:43 AM Last Updated: 8/17/2020 9:29 AM High Level Findings PTA/PIA ISCM FY2020 General ST&E Activities POA&Ms Accepted Risks System Artifacts SAP PAP ENERAL INFORMATION System ID CSAM ID: 2325 System Name Last Authorization Date: 4/1/2020 Division ATO Expiration Date: 4/1/2021 Compliant: 🔇 PIA SAOP Authorized Date: 9/30/201 System Operational Status (CSAM): Operation WebInspect VSA Start Date System Description: General Description tem contains the hardware and software required by t ping and maintaining, supporting the implementation of, overse ment and complying with applicable laws and regulations. Add The hardware of the 150-01 system consists of the following comp CUI//ISVI//FEDCON General Informa l Description/Purpose of Syste

### **Security Assessment Report**

### Sample Assessor & Management Dashboards

In Archer, role-based dashboards display task prioritization and management of A&A activities.



### **Assessor Dashboard**

### Management Dashboard

A&A Status - OISM Management - FY2020

Schedule	System	A&A Schedule Comment	A&A Status	Current Responsible	ATO Due Date 1	Personally Identifiable Information (PII)?	PIA Due to DOC	NIST: Primary Security Assessor (A&A)
Annual Assessment - Annual Assessment - FY2020			Authorized - Process Complete	A&A Coordinator	4/1/2020	Yes		Moore, Maureen
Annual Assessment - Annual Assessment - FY2020		Files need to be uploaded to CSAM.	Authorized - Process Complete	A&A Coordinator	4/1/2020	Yes		Vijayaverl, Rathini
Annual Assessment - Annual Assessment - FY2020		Files need to be uploaded to CSAM.	Authorized - Process Complete	A&A Coordinator	4/1/2020	Yes		Repaci, Jonathan

### **ISCM Status Tracker**



In Tableau, the Annual Assessment Progress report displays status of ISCM assessments by system.



# **Ongoing Authorization**



Historical data was evaluated to create initial risk thresholds in support of Ongoing Authorization decisions.

- Current threshold: NIST-wide Accepted Risk Average (all time)
- SOs and AOs can review a system's current security posture and risk trend:
  - Risk scores **at or below** the NIST average threshold could result in automatic reauthorization
  - Risk scores that **exceed** the threshold may require further review and discussion





# Aligning Privacy with CRS



Privacy capabilities have been integrated into the CRS Solution to standardize security and privacy processes across NIST.

### End users can complete the following privacy activities in CRS:

- Automate control assignments (NIST SP 800-53 Rev. 4, Appendix J.) for systems that contain PII
- Complete and generate on-demand DOC-required forms such as Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), and Annual Recertification
- Perform privacy control assessments and generate required documentation on-demand (Privacy Assessment Report and Privacy Assessment Plan)
- Quantify privacy risk based on CRS's scoring methodology

Privacy objectives (Predictability, Manageability, and Disassociability) scores are added together to calculate the Total Potential Risk for a single privacy control.

# Integrating CRS with Privacy

NIST

The following steps are completed in Archer for each system component to maintain privacy documentation and allocate applicable controls.





- A PTA is required for every system
- The **PTA** determines if a **PIA is** required
- CRS incorporates the current DOC PTA template

 The PIA collects information about the types of privacy data which is stored and processed, why it is collected, and how it is handled

**Complete PIA** 

• Privacy controls are allocated as determined by the PIA

### Generate Annual PIA Recertification Form





- The PIA recertification form is generated annually for ongoing authorization
- It also ensures that any changes to the Systems, Components, or privacy risks are identified and mitigated

## **PTA/PIA** Generation



The images below show the PTA and PIA Questionnaires ISSOs complete in Archer. Upon completion of the questionnaires, the PIA, PTA, and PIA Recertification forms are generated from Archer.

### **PTA and PIA Questionnaires**

▼ PIA GENERAL QUESTIO	INS										
PIA-	1: What is the statu	s of this information system?		O This is a new inform O This is an existing in create new privacy risk	ation system. formation system with cha 5.	nges that					
▼ INFORMATION IN TF For the below question Indicate when personally when personally	, i i i acheola	VENUMS	ns information system?		○ This is a new inform questions and complet O This is an existing in create new privey risk answer questions, and O This is an existing in do not create new priv approved Privacy Impa (Continue to answer que approved Privacy Impa (Continue to answer que do not create new priv approved Privacy Impa (Continue to answer que do not create new priv approved Privacy Impa Liter), Sip questions a Edit	ation system. (Continue to e certification.) formation system with cha La (Campitee chart below, co- complete certification.) formation system in which say risks, and there is a SA (Assessment (Continue to e certification.) formation system in which say risks, and there is a SA (Assessment (version 01- netrino and complete certification.)	answer nges that continue to changes SAOP o answer changes 2015). fication.) changes 2021 or				
<sup>€</sup> PIA-2.	V IT SYSTEM										
		PTA-2: Is the IT system or its in	nformation used to support an	y activity which may raise privacy concerns	? ⊖Yes ⊖No Edit		D				
		PTA-3: Does the IT system col	lect, maintain, or disseminate b	usiness identifiable information (BII)?	○ Yes, the IT system ci ○ No, this IT system di Edit	ollects, maintains, or disser oes not collect any BII.	minates BII.				
	PERSONALLY ID	ENTIFIABLE INFORMATION (PI	1)								
		PTA-4: Does the IT system col	lect, maintain, or disseminate p	ersonally identifiable information (PII)?	○ Yes, the IT system co ○ No, this IT system do Edit	ollects, maintains, or disser bes not collect any PII.	minates PII.				
	▼ PTA SUPPORTING ARTIFACTS   Add										
1	Name No Records Found	Size	Туре	Upload Date	Downloads	History					

### PIA, PTA, and PIA Recertification forms

U.S. Department	of Commerce Privacy Threshold A	nalysis						
National Institu	ite of Standards and Technology (N	(IST)						
Unique Project Identifie		Varia Masher 01 2010						
Introduction: This Priva		VESSOE POEMOEL 01-2019						
letermining if a Privacy I	U.S. Department of	f Commerce Privacy Impact Assessment						
rimarily based from the	National Institute	of Standards and Technology (NIST)						
Department of Commerce								
guidance is needed in ord Officer (BCPO).	Unique Project Identifier:							
Description of the inform	Introduction: System Des							
way that a non-technical								
following elements:	Provide a description of the	PRIVACY IMPACT ASSESSMENT (PIA)						
The E-Oovernment Act of 2002 define following is a summary of the definition		ANNUAL REVIEW CERTIFICATION FORM						
wocessing, maintenance, use, sharing,	<ul> <li>(a) whether it is a general s</li> <li>(b) System Investigation</li> </ul>	(Last SAOP approved PIA with updated signatures must accompany this form)						
) Whether it is a assure	(0) 33316m s0C0210H (a) Whather it is a standalay							
h) System location	deteribing one other cur							
) Whether it is a standa	(d) The way the system over							
describing any other s	(e) How information in the a							
<ol> <li>The purpose that the s</li> </ol>	(f) How information is trans							
<li>The way the system op</li>	(g) Any information sharing							
<ol> <li>A general description</li> </ol>	(h) The specific programma							
by the system	(i) The Federal Information							
z) Identify individuals w	system	Date of PIA Review: 09/28/2019						
<ul> <li>How information in th</li> <li>How information is to</li> </ul>		Name of System Owner: Couch. Charles						
y 110w byormation is br	a) Whether it is a general s							
a) Whether it is a gener	The Emergence Semicord	REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have						
-,	components: Physical Sec	reviewed the 11 system program and have confirmed that there have been no changes to the soutem reporter which securics rations the last SAOP approximatization of the PIA which is						
The Emergency Service	Gaithersburg, Visitor Res	currently posted on the Commerce website at commerce.doc.gov/privacy.						
components: Physical S System including Visite	Emergency Notification S							
and	provide the tools necessar	Signature of System Owner:						
Report Exec. These cor	security services for the p	Date of Privacy Act (PA) Review:						
mission to deliver emer	facilities.							
b) System location		Name of Reviewer: Fletcher, Catherine S., Privacy Act Officer						
The ENS component is	The ENS component is he	REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above.						
	located at the NIST Gaith	I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities,						
	continental United States.	SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the						
		currently posted on the Commerce website at commerce.doc.gov/privacy.						
	c) Whether it is a standalor	· ·						
	describing any other system	Signature of Privacy Act (PA) Reviewer:						
		Date of BCPO Review:						
		Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Schiller, Susannah						
		BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have						
		reviewed the security and privacy risks presented by the collection, processing, storage,						
		maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/program in the context of the current threat environment, along with any open Plane						
		of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in						
		privacy risks since the date that the PIA was last approved by the DOC SAOP.						
		Signature of the Bureau Chief Privacy Officer:						
		Jamary 2018						

### **Enterprise Management Dashboards**

## Enterprise System Security Dashboard

The Tableau dashboards supports NIST in maintaining ongoing awareness of information security and privacy to support organizational risk management decisions.



Data last refreshed from CRS on: 9/4/2020 6:51:16 AM

Sample Data

### Enterprise Vulnerability Trending Dashboard

The dashboard below summarizes the organization's active vulnerability trends over the past year.



### **Enterprise Vulnerabilities Dashboard**

The dashboard below summarizes vulnerability scan results by system and categorizes vulnerabilities by severity exposure.

![](_page_30_Figure_2.jpeg)

## Enterprise Secure Configuration Dashboard NST

The dashboard below summarizes secure configuration scan results by system and categorizes findings by severity and exposure.

![](_page_31_Figure_2.jpeg)

## Enterprise Web Vulnerability Dashboard

The dashboard below summarizes WebInspect scan results by system and indicates web application vulnerabilities by risk posture and severity.

![](_page_32_Figure_2.jpeg)

### Enterprise Asset Management Dashboard NST

The dashboard below displays the total number of assets within the organization and allows end users to search by CVE number to identify assets impacted by specific vulnerabilities.

![](_page_33_Figure_2.jpeg)

Sample Data

![](_page_34_Picture_1.jpeg)

### The dashboard below summarizes privacy risk metrics for system stakeholders.

![](_page_34_Figure_3.jpeg)

## **Cybersecurity Framework Dashboard**

The dashboard below represents the organization's performance against each function and category within the CSF.

	Cyberse	curi	ty Fra	mewo	rk (C	SF) v	iew o	of Ris	sk Ma	ana	geme	ent F	rame	wor	k (RI	MF)เ	ısing	) NIS	Т 80	0-53			
								Orga	anizati	onal F	ilters												
Advert Dear	Selet: Organiza	tional U	nit		Se	elect: Syst	tern					Select	: Compor	nents				Sele	ct: Gove	ernance		0	
Right	(AII)		• (A	JI)					*	(AJI)						*	(AII)				•		
to Observe In	npect																						/
		_							Rick	Filtors				_	_	_	_	_					
	-h Thursdald			- Di					NISK	- inter s		4.0.4				0-1					NI 07 04		
Ri:	sk Threshold	Sel	lect: Associ	ate Director	r 	S	elect: % S	atisfied		ZAID	Sele	ect: Categ	jory	_ 0	AID	Select: I	Function	_	Sel	ect Risk:	NISTV. SO	Respons	ible
1.3%	•	Allj			• (/	Ally			Ŧ	(All)				• 0	All)			•		responsible	e		*
Below Theo	schold Satisfied 100%																						
Meets Three	ishold																						
Function	Category																						
Identify	Asset Management (ID.AM)																				98.7%		
	Business Environment (ID.BE)																				98.8%		
	Governance (ID.GV)																				97.9%		
	Risk Assessment (ID.RA)																			91.9%			
	Risk Management Strategy (I																				100.0	%	
Protect	Access Control (PR.AC)																			91.7%			
	Awareness and Training (PR																				99.4%		
	Data Security (PR.DS)																			92.5%			
	Information Protection Proces.																			92.9%			
	Maintenance (PR.MA)																				100.0	%	
D. ( )	Protective Technology (PR.PT)	)																		94.7	%		
Detect	Anomalies and Events (DE.AE	)																			98.3%		
	Detection Processes (DE.DP)															72.0%							
Deenend	Security Continuous Monitorin.	·																		91.8%			
Respond	Analysis (RS.AN)																		0.40/		97.0%		
	Communications (RS.CO)																	8	0.4%		00.62		
	Improvements (RS.IM)																	00.000			99.1%		
	Mitigation (rt.S.MI) Response Planning (PC 20)																	82.9%			00.001		
Decover	Communications (RC CC)	_								_									_		98.9%		~
Recover	Communications (RC.CO)	0%	5% 10	% 15%	20%	25%	30%	35%	40%	45%	50%	55%	80%	85%	70%	75%	80%	85%	one:	05%	100%	105%	
		0.18	5/6 10	10/8	2076	2076	3076	5076	-10/0	- <del>1</del> 0/8 %	of Control	(s) Satisfied	i (Control)	50%	10/6	10/6	00.16	00 /8	80/6	80.6	100.76	10076	

NIST

# **Questions?**

![](_page_37_Picture_0.jpeg)

![](_page_37_Picture_1.jpeg)

Chris Enloe

Christian.Enloe@nist.gov

Sheldon Pratt

Sheldon.Pratt@nist.gov

Santi Kiran

Santi.Kiran@nist.gov

John Cascio

John.Cascio@nist.gov