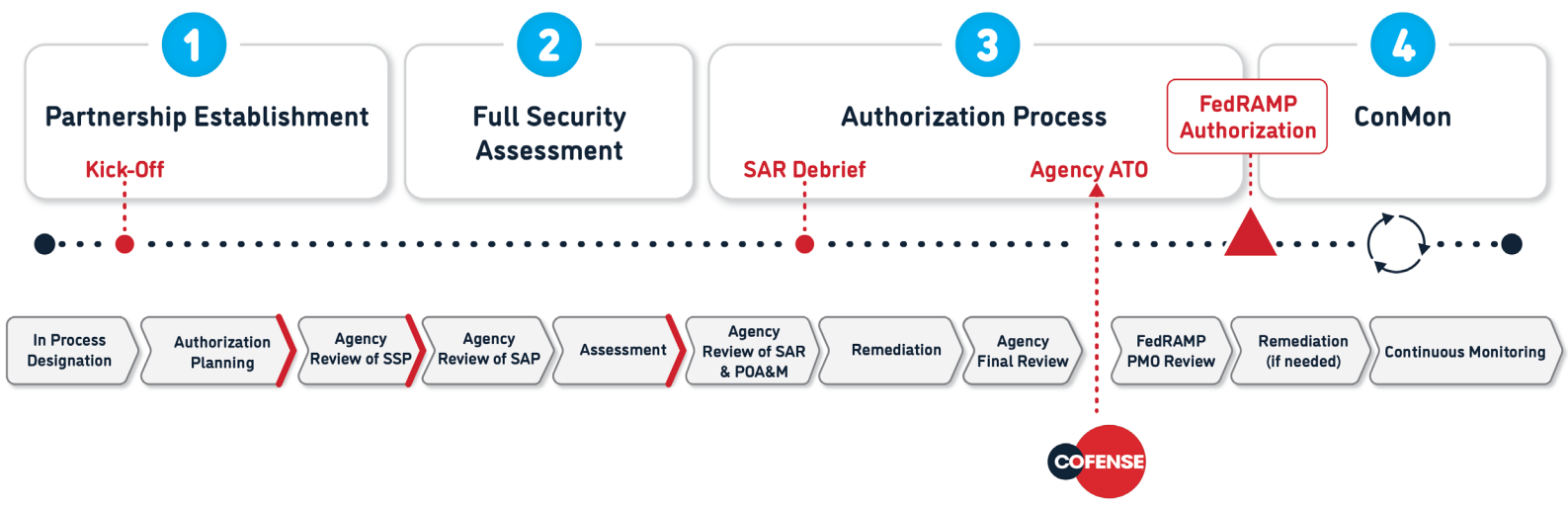
PHISHING DEFENSE FOR FEDERAL GOVERNMENT AGENCIES

As phishing threats rapidly evolve and increase, mission criticality must be your focus.

Spear phishing continues to be the most significant vulnerability among federal agencies. Are you confident your organization is prepared for an attack? Threat actors are targeting weaknesses such as social media, contracts and supply chains to infiltrate federal networks. In this "not if, but when" scenario, time is of the essence. Are you wasting precious time and effort in an ATO process for a non FedRAMP authorized vendor? Will your current phishing platform be FedRAMP Moderate authorized for 2021?

Cofense PhishMe is On Track to Achieving FedRAMP ATO-Moderate



Why Moderate Matters: The Rigorous Standards of FedRAMP 'Moderate' Authorization

Cofense PhishMe has received Agency Authority to Operate (ATO) from the US Department of Health and Human Services. We are getting closer to achieving ATO-Moderate for the FedRAMP "Moderate" Authorization. Our phishing awareness solution defends federal employees and the data they safeguard, including personally identifiable information, by conditioning them to spot and report phishing attacks. FedRAMP Moderate authorization has significantly stricter security controls than FedRAMP Low-Impact authorization, and Cofense PhishMe will meet the baseline for over 300 controls.

	KnowBe4	Cofense		
Control Type	**Li-Saas**	**Low**	**Moderate**	**High**
Access Control	4	11	43	54
Awareness Training	0	4	5	7
Adult and Accountability	3	10	10	30
Security Assessment and Authorization	5	9	16	16
Configuration Management	3	11	26	36
Contingency Planning	1	6	23	35
Identification and Authentication	6	15	27	32
Incident Response	2	7	17	26
Maintenance	0	4	12	14
Media Protection	0	4	10	12
Physical and Environment Protection	0	10	20	26
Planning	0	3	6	6
Personnel Security	1	8	9	10
Risk Assessment	3	4	10	12
System and Services Acquisition	1	6	22	26
System and Communication Protection	4	10	32	39
System and Information Integrity	3	7	28	38
TOTAL CONTROLS	**36**	**125**	**325**	**421**

ONLY COFENSE protects your agency with an end-to-end phishing defense.

Our solutions enable your teams to report, identify, and remove phishing attacks. Cofense delivers protection from malware threats, ransomware campaigns, and scams like sextortion which evade secure email gateways (SEGs) every day. Our solutions give federal teams the visibility and tools to stop phishing threats in minutes, not hours.

Cofense is a U.S. company, with a 100% U.S. management team and board, plus dedicated U.S.-based support staff. We have a well-established portfolio of federal government customers, enabling agencies to stop advanced phishing campaigns, fast.

Cofense Solutions

Condition Employees to Report Phishing

Federal agencies receive billions of weaponized emails each year. Cofense PhishMe and Reporter enable federal users to recognize and report the latest phishing threats. With input from our Intelligence, Research, and Phishing Defense teams, Cofense PhishMe simulates active threats that evade controls and land in user mailboxes. Our Reporter button is the easiest way for employees to report phishing. One click removes the email for SOC investigation. See why VA CIO Jim Gfrerer said, "We added our Cofense PhishMe button just in time".

Remove Phishing Campaigns with One Click

Users report suspicious emails. The SOC verifies. Now it's time to search and destroy. Cofense Vision empowers federal security teams to find phishing campaigns across their agency and remove them with one click. Run email searches instantly, without disrupting the mail team, while leaving an audit trail that keeps you in compliance. It's threat hunting at speed. Learn more at www.cofense.com/vision

Analyze and Respond to Attacks in Minutes

When federal users report emails, the SOC can't spend hours finding real threats in an ocean of noise. Cofense Triage automates noise reduction and email analysis, sending your SOC indicators of compromise in minutes. See why CSO.com called Triage "one of the most advanced defenses against phishing." Learn more at www.cofense.com/triage

> *"We know that in the midst of any crisis, threat actors are going to try to take advantage. Within our enterprise security program, we believe that the individual employee is probably both the strongest and weakest link, and so we put a lot of emphasis on education.* **We added our Cofense PhishMe button just in time.** *We put a lot of emphasis on making sure people are attuned to the cyber threats out there. The individual employee – it starts and ends with them."*
>
> — VA CIO Jim Gfrerer

ACT NOW

Find your peace of mind with Cofense solutions at www.cofense.com

COFENSE

W: cofense.com/contact **T:** 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175