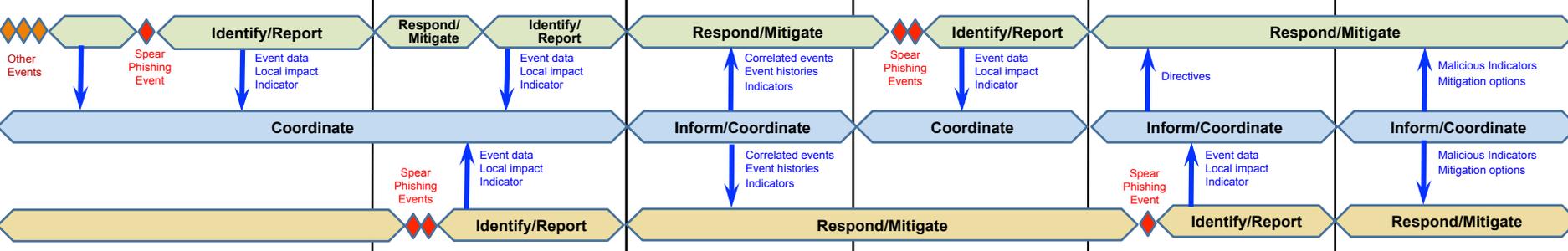




Many activities are happening concurrently in the D/A, US-CERT, and ISAC incident management operations as shown in this example cross-cutting spear phishing incident

 D/A	Identify/Report <ul style="list-style-type: none"> Detect spear phishing compromise Initiate D/A incident tracking Report indicator to US-CERT via the Cyber Indicators Repository (CIR) 	Identify/Report <ul style="list-style-type: none"> Take known affected users offline and warn others who received phishing email to delete it Identify/Report <ul style="list-style-type: none"> Investigate scope and impact Collaborate with US-CERT analyst 	Respond/Mitigate <ul style="list-style-type: none"> Extract observable indicators from EWIN or CIR Update block lists and sensors 	Response/Mitigate <ul style="list-style-type: none"> Monitor for suspicious activities Alert users to watch for and report suspicious emails Identify/Report <ul style="list-style-type: none"> Report new observed indicators 	Respond/Mitigate <ul style="list-style-type: none"> Coordinate with US-CERT management to understand threat Prioritize resources to complete directive actions 	Respond/Mitigate <ul style="list-style-type: none"> Extract observable indicators from SAR to monitor for suspicious activity Update block lists and sensors Implement recommended defensive measures and best practices 	
	Coordinate <ul style="list-style-type: none"> Acknowledge indicators from D/A 	Coordinate <ul style="list-style-type: none"> Collaborate with D/A to corroborate and analyze findings Investigate incident scope, timeline Discover other affected D/As 	Inform/Coordinate <ul style="list-style-type: none"> Communicate initial analysis of the threat via Early Warning and Indicator Notice (EWIN) or CIR to D/As, and via EWIN to ISACs 	Coordinate <ul style="list-style-type: none"> Receive new indicators from GFIRST community Discover Fast Flux network in a serious targeted campaign Escalate to internal management 	Inform/Coordinate <ul style="list-style-type: none"> Coordinate with D/A management to prioritize resources 	Inform/Coordinate <ul style="list-style-type: none"> Communicate broad assessment of threat and actionable recommendations via Security Awareness Report (SAR) to D/As, and via Critical Infrastructure Information Notice (CIIN) to ISACs 	
	Normal ISAC Activity	Identify/Report <ul style="list-style-type: none"> ISAC members detect phishing compromise Report indicator to US-CERT Investigate scope, impact across ISAC members 	Respond/Mitigate <ul style="list-style-type: none"> Coordinate ISAC members' response Analyze EWIN related data Initiate effectiveness monitoring across members 	Response/Mitigate <ul style="list-style-type: none"> Host conference call with members to follow up on the EWIN 	Identify/Report <ul style="list-style-type: none"> Report to US-CERT new indicator received from ISAC members 	Respond/Mitigate <ul style="list-style-type: none"> Coordinate ISAC members' response Analyze CIIN related data Initiate effective monitoring across members 	



Acronyms:
 CIR – Cyber Indicators Repository
 EWIN - Early Warning and Indicator Notice
 SAR – Security Awareness Report
 CIIN - Critical Infrastructure Information Notice