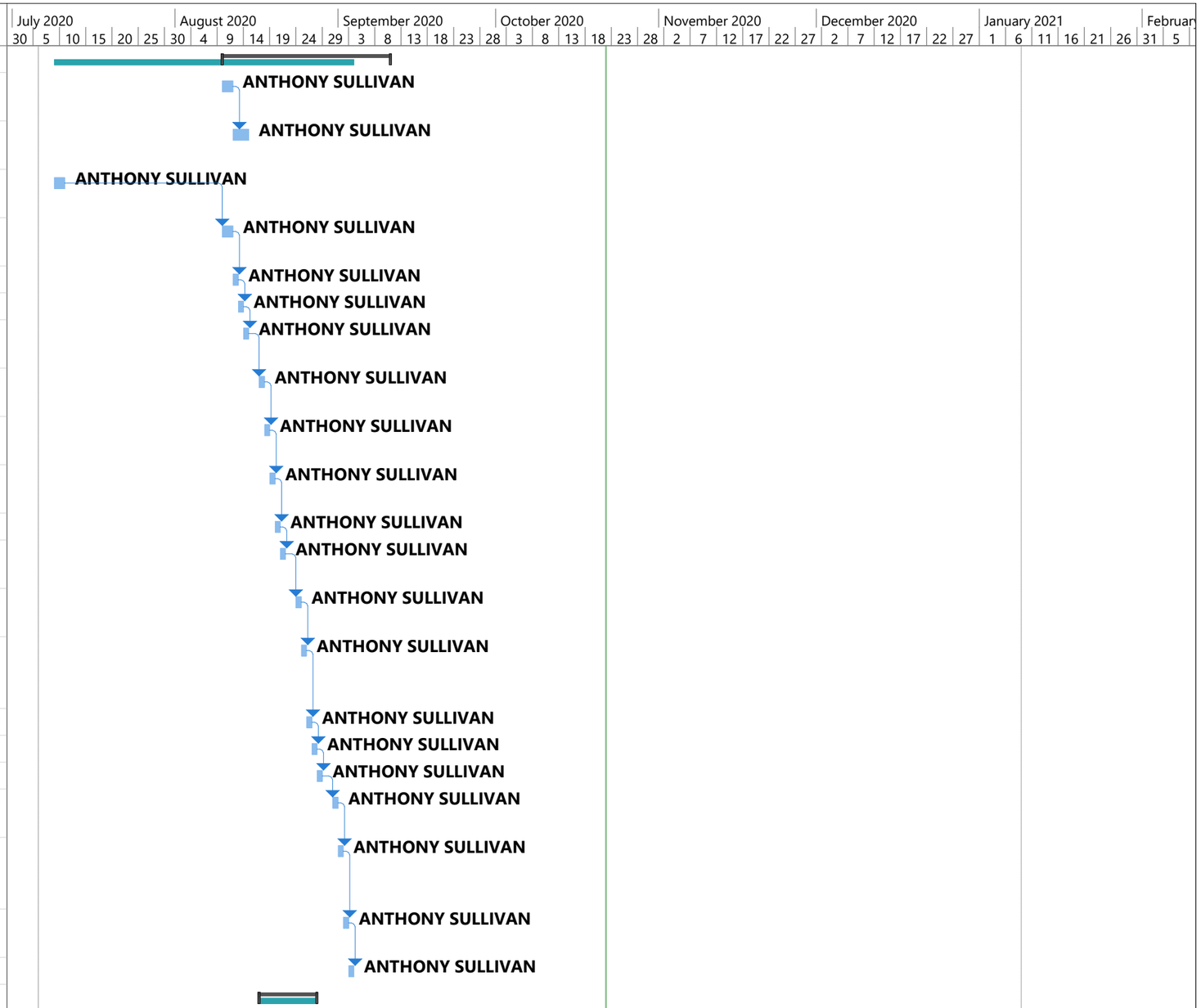
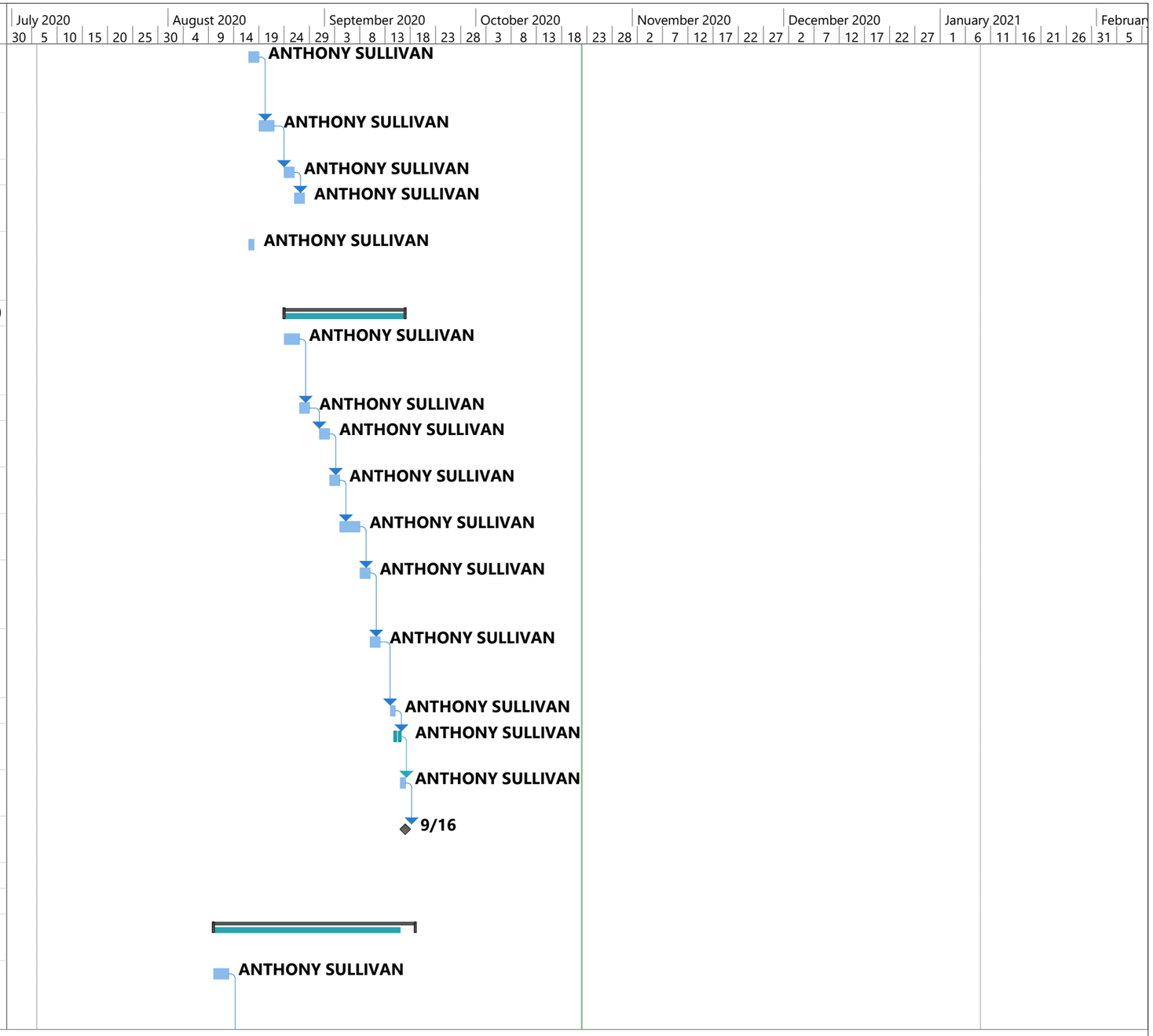
ID	Task Mode	Task Name	Duration	Start	Finish
1		**Asset management (ID.AM)**	**24 days**	**Mon 8/10/20**	**Thu 9/10/20**
2		AC-1 ACCESS CONTROL POLICY AND PROCEDURES P1	2 days	Mon 8/10/20	Tue 8/11/20
3		AC-2 ACCOUNT MANAGEMENT P1	3 days	Wed 8/12/20	Fri 8/14/20
4		AC-3 ACCESS ENFORCEMENT P1	2 days	Thu 7/9/20	Fri 7/10/20
5		AC-4 INFORMATION FLOW ENFORCEMENT P1	2 days	Mon 8/10/20	Tue 8/11/20
6		AC-5 SEPARATION OF DUTIES	1 day	Wed 8/12/20	Wed 8/12/20
7		AC-6 LEAST PRIVILEGE P1	1 day	Thu 8/13/20	Thu 8/13/20
8		AC-7 UNSUCCESSFUL LOGIN ATTEMPTS P2	1 day	Fri 8/14/20	Fri 8/14/20
9		AC-8 SYSTEM USE NOTIFICATION P1	1 day	Mon 8/17/20	Mon 8/17/20
10		AC-9 PREVIOUS LOGON NOTIFICATION P0	1 day	Tue 8/18/20	Tue 8/18/20
11		AC-10 CONCURRENT SESSION CONTROL P3	1 day	Wed 8/19/20	Wed 8/19/20
12		AC-11 SESSION LOCK P3	1 day	Thu 8/20/20	Thu 8/20/20
13		AC-12 SESSION TERMINATION P2	1 day	Fri 8/21/20	Fri 8/21/20
14		AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL	1 day	Mon 8/24/20	Mon 8/24/20
15		AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION P3	1 day	Tue 8/25/20	Tue 8/25/20
16		AC-15 AUTOMATED MARKING	1 day	Wed 8/26/20	Wed 8/26/20
17		AC-16 AUTOMATED LABELING	1 day	Thu 8/27/20	Thu 8/27/20
18		AC-17 REMOTE ACCESS P1	1 day	Fri 8/28/20	Fri 8/28/20
19		AC-18 WIRELESS ACCESS RESTRICTIONS P1	1 day	Mon 8/31/20	Mon 8/31/20
20		AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES P1	1 day	Tue 9/1/20	Tue 9/1/20
21		AC-20 USE OF EXTERNAL INFORMATION SYSTEMS P1	1 day	Wed 9/2/20	Wed 9/2/20
22		ACCESS CONTROLS COMPLETE	1 day	Thu 9/3/20	Thu 9/3/20
24		**AWARENESS AND TRAINING**	**9 days**	**Mon 8/17/20**	**Thu 8/27/20**



Project: MASTER PLAN
Date: Thu 10/22/20

Task	Project Summary	Manual Task	Start-only	Deadline	
Split	Inactive Task	Duration-only	Finish-only	Progress	
Milestone	Inactive Milestone	Manual Summary Rollup	External Tasks	Manual Progress	
Summary	Inactive Summary	Manual Summary	External Milestone		

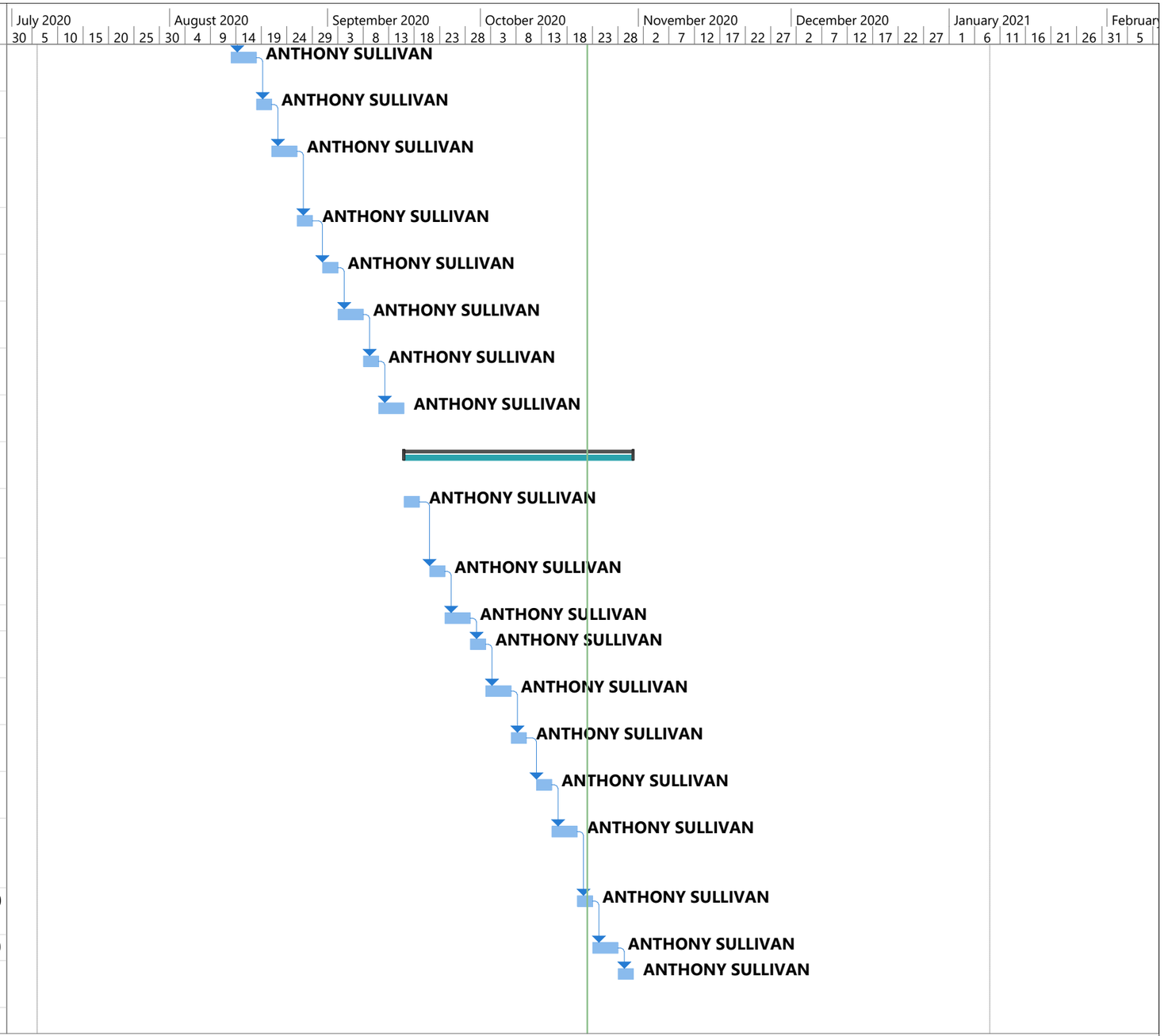
ID	Task Mode	Task Name	Duration	Start	Finish
25		AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES P1	2 days	Mon 8/17/20	Tue 8/18/20
26		AT-2 SECURITY AWARENESS P1	3 days	Wed 8/19/20	Fri 8/21/20
27		AT-3 SECURITY TRAINING P1	2 days	Mon 8/24/20	Tue 8/25/20
28		AT-4 SECURITY TRAINING RECORDS P3	2 days	Wed 8/26/20	Thu 8/27/20
29		AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS P0	1 day	Mon 8/17/20	Mon 8/17/20
30		**AUDIT AND ACCOUNTABILITY**	**18 days**	**Mon 8/24/20**	**Wed 9/16/20**
31		AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES P1	3 days	Mon 8/24/20	Wed 8/26/20
32		AU-2 AUDITABLE EVENTS P1	2 days	Thu 8/27/20	Fri 8/28/20
33		AU-3 CONTENT OF AUDIT RECORDS P1	2 days	Mon 8/31/20	Tue 9/1/20
34		AU-4 AUDIT STORAGE CAPACITY P1	2 days	Wed 9/2/20	Thu 9/3/20
35		AU-5 RESPONSE TO AUDIT PROCESSING FAILURES P1	2 days	Fri 9/4/20	Mon 9/7/20
36		AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING P1	2 days	Tue 9/8/20	Wed 9/9/20
37		AU-7 AUDIT REDUCTION AND REPORT GENERATION P2	2 days	Thu 9/10/20	Fri 9/11/20
38		AU-8 TIME STAMPS P1	1 day	Mon 9/14/20	Mon 9/14/20
39		AU-9 PROTECTION OF AUDIT INFORMATION P1	1 day	Tue 9/15/20	Tue 9/15/20
40		AU-10 NON-REPUDIATION P2	1 day	Wed 9/16/20	Wed 9/16/20
41		AUDIT AND ACCOUNTABILITY Complete	0 days	Wed 9/16/20	Wed 9/16/20
42		<New Task>			
43					
44		**SECURITY ASSESSMENT AND AUTHORIZATION**	**30 days?**	**Mon 8/10/20**	**Fri 9/18/20**
45		CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES P1	3 days	Mon 8/10/20	Wed 8/12/20



Project: MASTER PLAN
Date: Thu 10/22/20

Task	Project Summary	Manual Task	Start-only	Deadline	
Split	Inactive Task	Duration-only	Finish-only	Progress	
Milestone	Inactive Milestone	Manual Summary Rollup	External Tasks	Manual Progress	
Summary	Inactive Summary	Manual Summary	External Milestone		

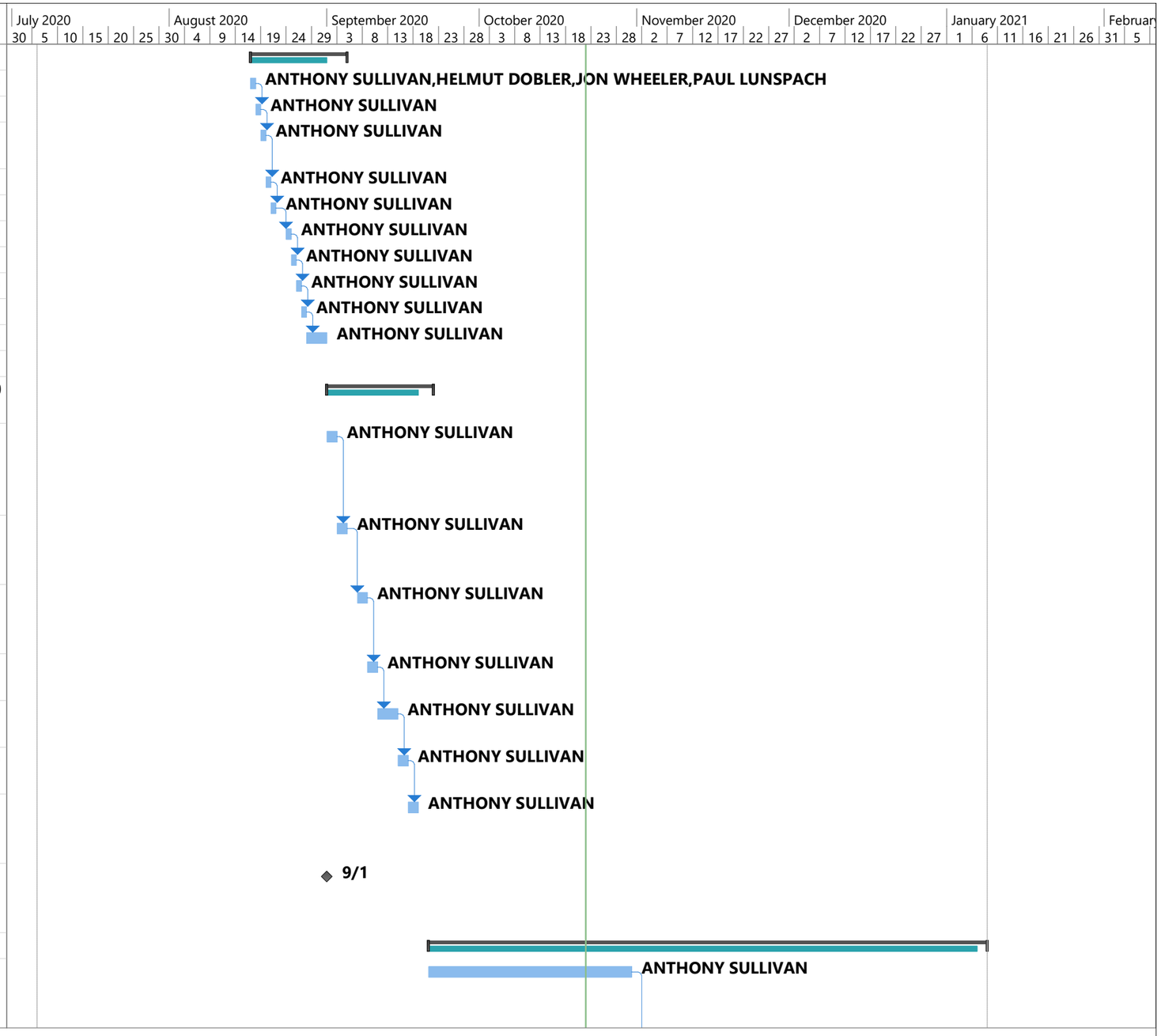
ID	Task Mode	Task Name	Duration	Start	Finish
46		CA-2 SECURITY ASSESSMENTS P2	3 days	Thu 8/13/20	Mon 8/17/20
47		CA-3 SYSTEM INTERCONNECTIONS P1	3 days	Tue 8/18/20	Thu 8/20/20
48		CA-4 SECURITY CERTIFICATION WITHDRAWN	3 days	Fri 8/21/20	Tue 8/25/20
49		CA-5 PLAN OF ACTION AND MILESTONES P3	3 days	Wed 8/26/20	Fri 8/28/20
50		CA-6 SECURITY AUTHORIZATION P2	3 days	Mon 8/31/20	Wed 9/2/20
51		CA-7 CONTINUOUS MONITORING P2	3 days	Thu 9/3/20	Mon 9/7/20
52		CA-8 PENETRATION TESTING P2	3 days	Tue 9/8/20	Thu 9/10/20
53		CA-9 INTERNAL SYSTEM CONNECTIONS P2	3 days	Fri 9/11/20	Tue 9/15/20
54		**CONFIGURATION MANAGEMENT**	**33 days?**	**Wed 9/16/20**	**Fri 10/30/20**
55		CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES P1	3 days	Wed 9/16/20	Fri 9/18/20
56		CM-2 BASELINE CONFIGURATION P1	3 days	Mon 9/21/20	Wed 9/23/20
57		CM-3 CONFIGURATION CHANGE	3 days	Thu 9/24/20	Mon 9/28/20
58		CM-4 SECURITY IMPACT ANALYSIS P2	3 days	Tue 9/29/20	Thu 10/1/20
59		CM-5 ACCESS RESTRICTIONS FOR CHANGE P1	3 days	Fri 10/2/20	Tue 10/6/20
60		CM-6 CONFIGURATION SETTINGS P1	3 days	Wed 10/7/20	Fri 10/9/20
61		CM-7 LEAST FUNCTIONALITY P1	3 days	Mon 10/12/20	Wed 10/14/20
62		CM-8 INFORMATION SYSTEM COMPONENT INVENTORY P1	3 days	Thu 10/15/20	Mon 10/19/20
63		CM-9 CONFIGURATION MANAGEMENT PLAN P1	3 days	Tue 10/20/20	Thu 10/22/20
64		CM-10 SOFTWARE USAGE RESTRI	3 days	Fri 10/23/20	Tue 10/27/20
65		CM-11 USER-INSTALLED SOFTWARE P1	3 days	Wed 10/28/20	Fri 10/30/20
66					



Project: MASTER PLAN
Date: Thu 10/22/20

Task	Project Summary	Manual Task	Start-only	Deadline	
Split	Inactive Task	Duration-only	Finish-only	Progress	
Milestone	Inactive Milestone	Manual Summary Rollup	External Tasks	Manual Progress	
Summary	Inactive Summary	Manual Summary	External Milestone		

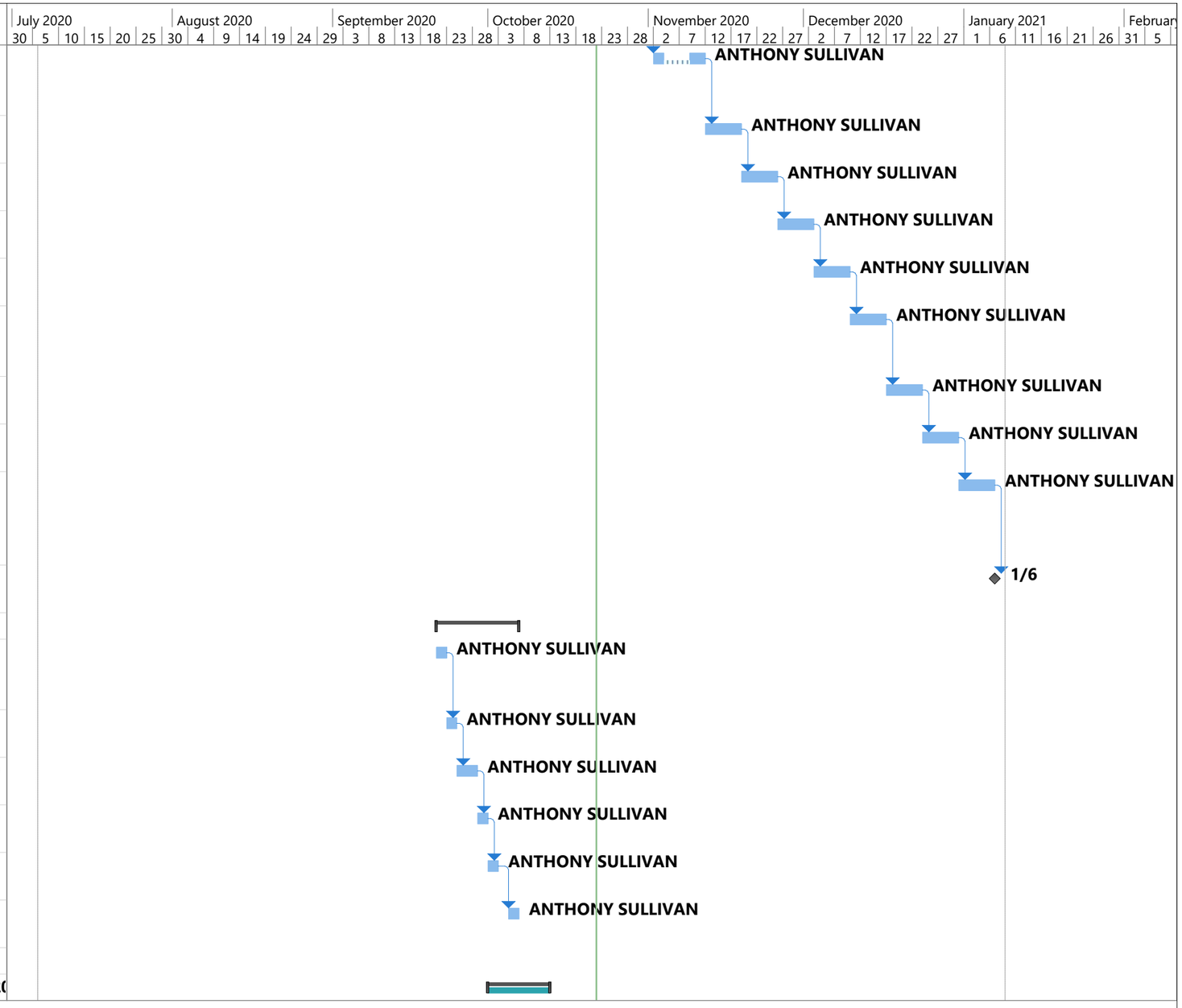
ID	Task Mode	Task Name	Duration	Start	Finish
67		**CONTINGENCY PLANNING**	**15 days**	**Mon 8/17/20**	**Fri 9/4/20**
68		CP-1 CONTINGENCY PLANNING P	1 day	Mon 8/17/20	Mon 8/17/20
69		CP-2 CONTINGENCY PLAN P1	1 day	Tue 8/18/20	Tue 8/18/20
70		CP-3 CONTINGENCY TRAINING P2	1 day	Wed 8/19/20	Wed 8/19/20
71		CP-4 CONTINGENCY PLAN TESTIN	1 day	Thu 8/20/20	Thu 8/20/20
72		CP-5 CONTINGENCY PLAN UPDAT	1 day	Fri 8/21/20	Fri 8/21/20
73		CP-6 ALTERNATE STORAGE SITE P	1 day	Mon 8/24/20	Mon 8/24/20
74		CP-7 ALTERNATE PROCESSING SI	1 day	Tue 8/25/20	Tue 8/25/20
75		CP-8 TELECOMMUNICATIONS SEI	1 day	Wed 8/26/20	Wed 8/26/20
76		CP-9 INFORMATION SYSTEM BAC	1 day	Thu 8/27/20	Thu 8/27/20
77		CP-10 INFORMATION SYSTEM RE	2 days	Fri 8/28/20	Mon 8/31/20
78					
79		**IDENTIFICATION AND AUTHENTICATION**	**15 days**	**Tue 9/1/20**	**Mon 9/21/20**
80		IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES P1	2 days	Tue 9/1/20	Wed 9/2/20
81		IA-2 USER IDENTIFICATION AND AUTHENTICATION P1	2 days	Thu 9/3/20	Fri 9/4/20
82		IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION P1	2 days	Mon 9/7/20	Tue 9/8/20
83		IA-4 IDENTIFIER MANAGEMENT P1	2 days	Wed 9/9/20	Thu 9/10/20
84		IA-5 AUTHENTICATOR MANAGEMENT P1	2 days	Fri 9/11/20	Mon 9/14/20
85		IA-6 AUTHENTICATOR FEEDBACK P2	2 days	Tue 9/15/20	Wed 9/16/20
86		IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION P1	2 days	Thu 9/17/20	Fri 9/18/20
87		IDENTIFICATION AND AUTHENTICATION COMPLETE	0 days	Tue 9/1/20	Tue 9/1/20
89		**INCIDENT RESPONSE**	**80 days?**	**Mon 9/21/20**	**Fri 1/8/21**
90		IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES P1	30 days	Mon 9/21/20	Fri 10/30/20



Project: MASTER PLAN
Date: Thu 10/22/20

Task	Project Summary	Manual Task	Start-only	Deadline	
Split	Inactive Task	Duration-only	Finish-only	Progress	
Milestone	Inactive Milestone	Manual Summary Rollup	External Tasks	Manual Progress	
Summary	Inactive Summary	Manual Summary	External Milestone		

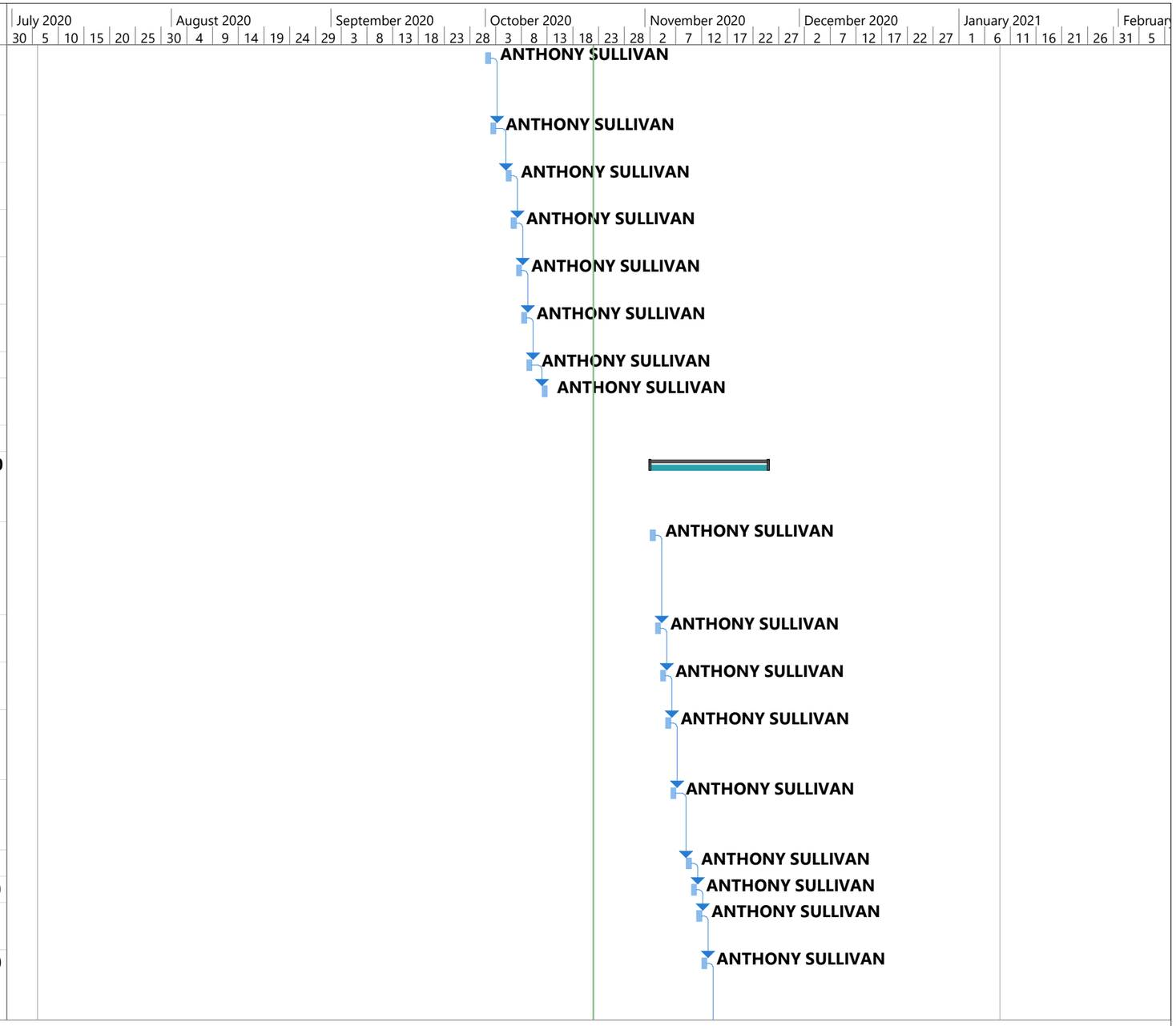
ID	Task Mode	Task Name	Duration	Start	Finish
91		IR-2 INCIDENT RESPONSE TRAINING P1	5 days	Mon 11/2/20	Wed 11/11/20
92		IR-3 INCIDENT RESPONSE TESTING P1	5 days	Thu 11/12/20	Wed 11/18/20
93		IR-4 INCIDENT HANDLING P1	5 days	Thu 11/19/20	Wed 11/25/20
94		IR-5 INCIDENT MONITORING P1	5 days	Thu 11/26/20	Wed 12/2/20
95		IR-6 INCIDENT REPORTING P1	5 days	Thu 12/3/20	Wed 12/9/20
96		IR-7 INCIDENT RESPONSE ASSISTANCE P2	5 days	Thu 12/10/20	Wed 12/16/20
97		IR-8 INCIDENT RESPONSE PLAN P1	5 days	Thu 12/17/20	Wed 12/23/20
98		IR-9 INFORMATION SPILLAGE RESPONSE P1	5 days	Thu 12/24/20	Wed 12/30/20
99		IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM P1	5 days	Thu 12/31/20	Wed 1/6/21
100		INCIDENT RESPONSE COMPLETE	0 days	Wed 1/6/21	Wed 1/6/21
102		**MAINTENANCE**	**12 days**	**Mon 9/21/20**	**Tue 10/6/20**
103		MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES P1	2 days	Mon 9/21/20	Tue 9/22/20
104		MA-2 CONTROLLED MAINTENANCE P1	2 days	Wed 9/23/20	Thu 9/24/20
105		MA-3 MAINTENANCE TOOLS P2	2 days	Fri 9/25/20	Mon 9/28/20
106		MA-4 NONLOCAL MAINTENANCE P2	2 days	Tue 9/29/20	Wed 9/30/20
107		MA-5 MAINTENANCE PERSONNEL P2	2 days	Thu 10/1/20	Fri 10/2/20
108		MA-6 TIMELY MAINTENANCE P2	2 days	Mon 10/5/20	Tue 10/6/20
109					
110		**MEDIA PROTECTION**	**8 days?**	**Thu 10/1/20**	**Mon 10/12/20**



Project: MASTER PLAN
Date: Thu 10/22/20

Task	Project Summary	Manual Task	Start-only	Deadline
Split	Inactive Task	Duration-only	Finish-only	Progress
Milestone	Inactive Milestone	Manual Summary Rollup	External Tasks	Manual Progress
Summary	Inactive Summary	Manual Summary	External Milestone

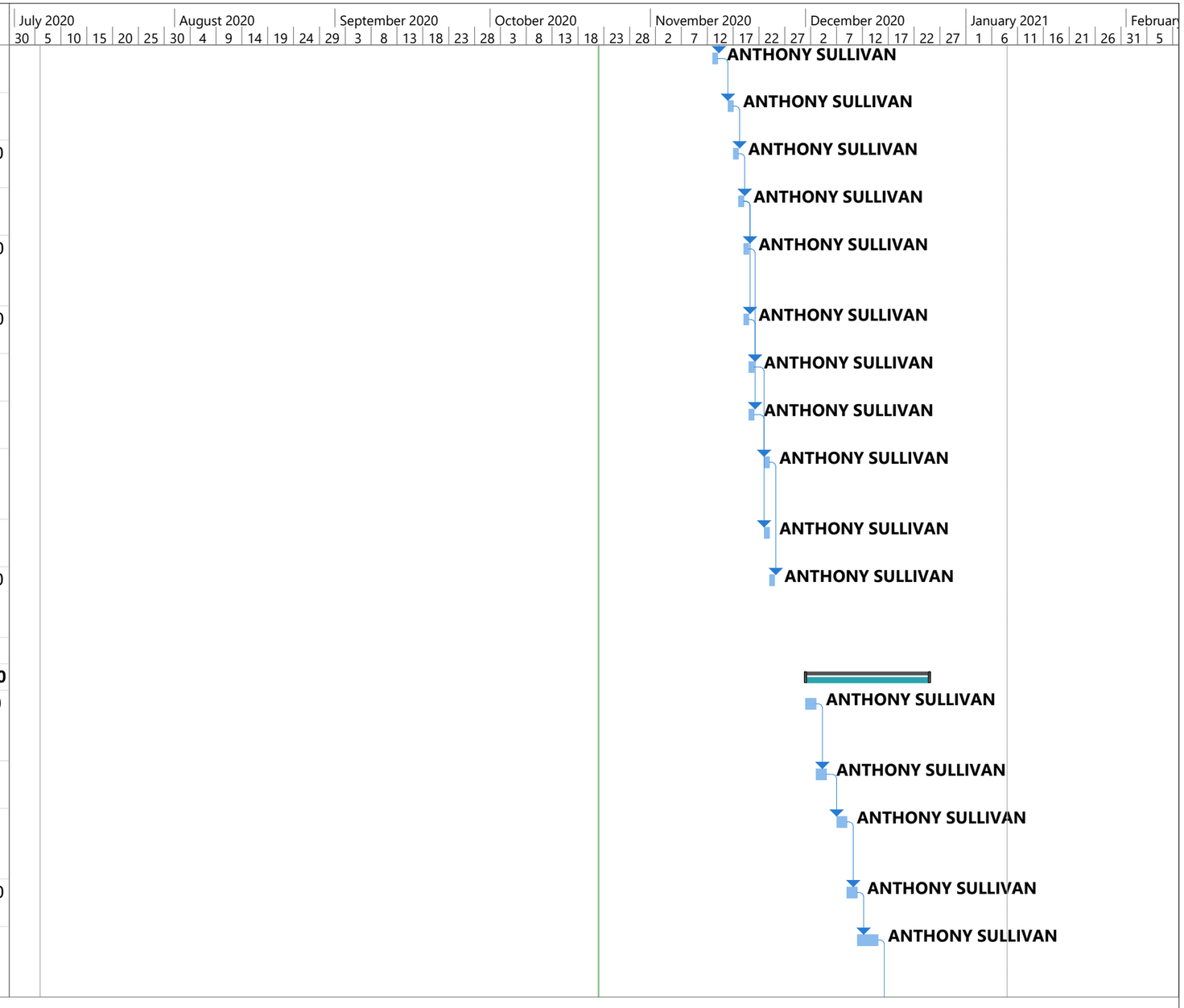
ID	Task Mode	Task Name	Duration	Start	Finish
111		MP-1 MEDIA PROTECTION POLICY AND PROCEDURES P1	1 day?	Thu 10/1/20	Thu 10/1/20
112		MP-2 MEDIA ACCESS P1	1 day?	Fri 10/2/20	Fri 10/2/20
113		MP-3 MEDIA MARKING P2	1 day?	Mon 10/5/20	Mon 10/5/20
114		MP-4 MEDIA STORAGE P1	1 day?	Tue 10/6/20	Tue 10/6/20
115		MP-5 MEDIA TRANSPORT P1	1 day?	Wed 10/7/20	Wed 10/7/20
116		MP-6 MEDIA SANITIZATION P1	1 day?	Thu 10/8/20	Thu 10/8/20
117		MP-7 MEDIA USE P1	1 day?	Fri 10/9/20	Fri 10/9/20
118		MP-8 MEDIA DOWNGRADING P1	1 day?	Mon 10/12/20	Mon 10/12/20
119					
120		**PHYSICAL AND ENVIRONMENTAL PROTECTION**	**17 days?**	**Mon 11/2/20**	**Tue 11/24/20**
121		PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES P1	1 day	Mon 11/2/20	Mon 11/2/20
122		PE-2 PHYSICAL ACCESS AUTHORIZATIONS P1	1 day	Tue 11/3/20	Tue 11/3/20
123		PE-3 PHYSICAL ACCESS CONTROL P1	1 day	Wed 11/4/20	Wed 11/4/20
124		PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM P1	1 day	Thu 11/5/20	Thu 11/5/20
125		PE-5 ACCESS CONTROL FOR OUTPUT DEVICES P2	1 day	Fri 11/6/20	Fri 11/6/20
126		PE-6 MONITORING PHYSICAL ACC	1 day	Mon 11/9/20	Mon 11/9/20
127		PE-7 VISITOR CONTROL	1 day	Tue 11/10/20	Tue 11/10/20
128		PE-8 VISITOR ACCESS RECORDS P3	1 day	Wed 11/11/20	Wed 11/11/20
129		PE-9 POWER EQUIPMENT AND CABLING P1	1 day	Thu 11/12/20	Thu 11/12/20



Project: MASTER PLAN
Date: Thu 10/22/20

Task	Project Summary	Manual Task	Start-only	Deadline
Split	Inactive Task	Duration-only	Finish-only	Progress
Milestone	Inactive Milestone	Manual Summary Rollup	External Tasks	Manual Progress
Summary	Inactive Summary	Manual Summary	External Milestone

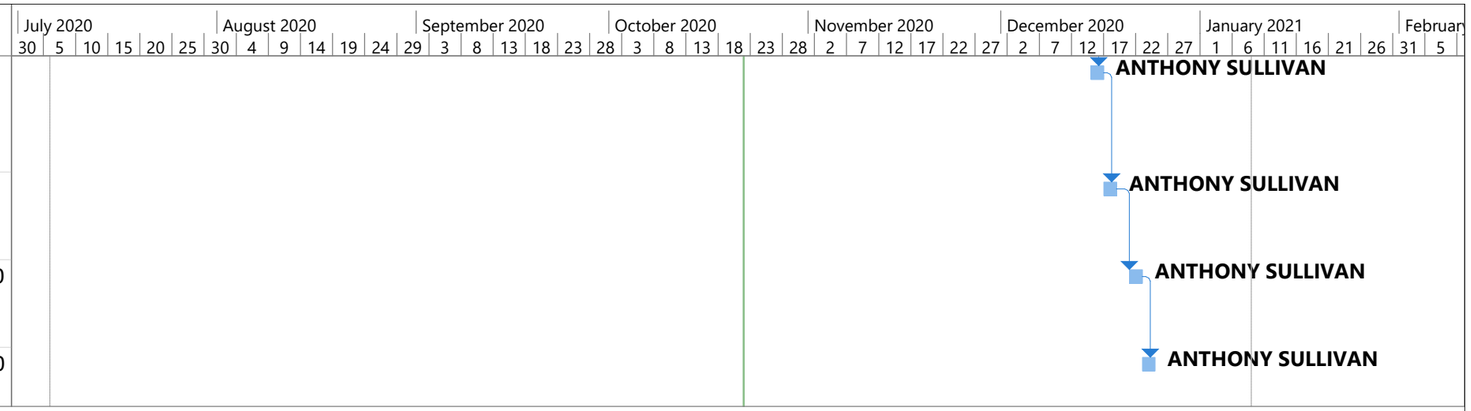
ID	Task Mode	Task Name	Duration	Start	Finish
130		PE-10 EMERGENCY SHUTOFF P1	1 day	Fri 11/13/20	Fri 11/13/20
131		PE-11 EMERGENCY POWER P1	1 day	Mon 11/16/20	Mon 11/16/20
132		PE-12 EMERGENCY LIGHTING P1	1 day	Tue 11/17/20	Tue 11/17/20
133		PE-13 FIRE PROTECTION P1	1 day	Wed 11/18/20	Wed 11/18/20
134		PE-14 TEMPERATURE AND HUMIDITY CONTROLS P1	1 day	Thu 11/19/20	Thu 11/19/20
135		PE-15 WATER DAMAGE PROTECTION P1	1 day	Thu 11/19/20	Thu 11/19/20
136		PE-16 DELIVERY AND REMOVAL P2	1 day	Fri 11/20/20	Fri 11/20/20
137		PE-17 ALTERNATE WORK SITE P2	1 day	Fri 11/20/20	Fri 11/20/20
138		PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS P3	1 day	Mon 11/23/20	Mon 11/23/20
139		PE-19 INFORMATION LEAKAGE P0	1 day	Mon 11/23/20	Mon 11/23/20
140		PE-20 ASSET MONITORING AND TRACKING P0	1 day	Tue 11/24/20	Tue 11/24/20
141					
142		**PLANNING**	**18 days?**	**Tue 12/1/20**	**Thu 12/24/20**
143		PL-1 SECURITY PLANNING POLICY AND PROCEDURES P1	2 days	Tue 12/1/20	Wed 12/2/20
144		PL-2 SYSTEM SECURITY PLAN P1	2 days	Thu 12/3/20	Fri 12/4/20
145		PL-3 SYSTEM SECURITY PLAN UPDATE WITHDRAWN	2 days	Mon 12/7/20	Tue 12/8/20
146		PL-4 RULES OF BEHAVIOR P2	2 days	Wed 12/9/20	Thu 12/10/20
147		PL-5 PRIVACY IMPACT ASSESSMENT WITHDRAWN	2 days	Fri 12/11/20	Mon 12/14/20



Project: MASTER PLAN
Date: Thu 10/22/20

Task	Project Summary	Manual Task	Start-only	Deadline			
Split	Inactive Task	Duration-only	Finish-only	Progress			
Milestone	Inactive Milestone	Manual Summary Rollup	External Tasks	Manual Progress			
Summary	Inactive Summary	Manual Summary	External Milestone				

ID	Task Mode	Task Name	Duration	Start	Finish
148		PL-6 SECURITY-RELATED ACTIVITY PLANNING WITHDRAWN	2 days	Tue 12/15/20	Wed 12/16/20
149		PL-7 SECURITY CONCEPT OF OPERATIONS P1	2 days	Thu 12/17/20	Fri 12/18/20
150		PL-8 INFORMATION SECURITY ARCHITECTURE P1	2 days	Mon 12/21/20	Tue 12/22/20
151		PL-9 CENTRAL MANAGEMENT P0	2 days	Wed 12/23/20	Thu 12/24/20



Project: MASTER PLAN
Date: Thu 10/22/20

Task	Project Summary	Manual Task	Start-only	Deadline
Split	Inactive Task	Duration-only	Finish-only	Progress
Milestone	Inactive Milestone	Manual Summary Rollup	External Tasks	Manual Progress
Summary	Inactive Summary	Manual Summary	External Milestone	

1 **Asset management (ID.AM)**

This is a summary task. Use summary tasks to help organize your project into sections.

2 **AC-1 ACCESS CONTROL POLICY AND PROCEDURES P1**

AC-1	ACCESS CONTROL POLICY AND PROCEDURES	LOW	P1	Access Control

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

3 **AC-2 ACCOUNT MANAGEMENT P1**

AC-2	ACCOUNT MANAGEMENT	LOW	P1	Access Control

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts.
Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.

Control Enhancements:

(1) The organization employs automated mechanisms to support the management of information system accounts.

(2) The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].

(3) The information system automatically disables inactive accounts after [*Assignment: organization- defined time period*].

(4) The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

LOW AC-2	**MOD** AC-2 (1) (2) (3) (4)	**HIGH** AC-2 (1) (2) (3) (4)

4 **AC-3 ACCESS ENFORCEMENT P1**

AC-3	ACCESS ENFORCEMENT	LOW	P1	Access Control

AC-3 ACCESS ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. Related security control: SC-13.

Control Enhancements:

(1) The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Enhancement Supplemental Guidance: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users.
Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

LOW AC-3	**MOD** AC-3 (1)	**HIGH** AC-3 (1)

5 AC-4 INFORMATION FLOW ENFORCEMENT P1

AC-4	INFORMATION FLOW ENFORCEMENT	MODERATE	P1	Access Control

AC-4 INFORMATION FLOW ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Related security control: SC-7.

Control Enhancements:

(1) The information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions.

Enhancement Supplemental Guidance: Information flow control enforcement using explicit labels is used, for example, to control the release of certain types of information.

(2) The information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.

(3) The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.

LOW Not Selected	**MOD** AC-4	**HIGH** AC-4

6 AC-5 SEPARATION OF DUTIES

AC-5 SEPARATION OF DUTIES

Control: The information system enforces separation of duties through assigned access authorizations.

Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-5	**HIGH** AC-5

7 AC-6 LEAST PRIVILEGE P1

AC-6	LEAST PRIVILEGE	MODERATE	P1	Access Control

AC-6 LEAST PRIVILEGE

Control: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Supplemental Guidance: The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-6	**HIGH** AC-6

8 AC-7 UNSUCCESSFUL LOGIN ATTEMPTS P2

AC-7	UNSUCCESSFUL LOGON ATTEMPTS	LOW	P2	Access Control

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period. The information system automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*], *delays next login prompt according to Assignment: organization-defined delay algorithm.*]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Control Enhancements:

(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

LOW AC-7	**MOD** AC-7	**HIGH** AC-7

9 AC-8 SYSTEM USE NOTIFICATION P1

AC-8	SYSTEM USE NOTIFICATION	LOW	P1	Access Control

AC-8 SYSTEM USE NOTIFICATION

Control: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
(iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Supplemental Guidance: Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Control Enhancements: None.

LOW AC-8	**MOD** AC-8	**HIGH** AC-8

10 AC-9 PREVIOUS LOGON NOTIFICATION P0

AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION		P0	Access Control

AC-9 PREVIOUS LOGON NOTIFICATION

Control: The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

11 AC-10 CONCURRENT SESSION CONTROL P3

AC-10 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for any user to [*Assignment: organization-defined number of sessions*].

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** AC-10

12 AC-11 SESSION LOCK P3

AC-11 SESSION LOCK

Control: The information system prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Supplemental Guidance: Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-11	**HIGH** AC-11

13 AC-12 SESSION TERMINATION P2

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a remote session after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: A remote session is initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non- organization-controlled network (e.g., the Internet).

Control Enhancements:

(1) Automatic session termination applies to local and remote sessions.

LOW Not Selected	**MOD** AC-12	**HIGH** AC-12 (1)

14 AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the review of user activities.

LOW AC-13	**MOD** AC-13 (1)	**HIGH** AC-13 (1)

15 AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION P3

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.

Supplemental Guidance: The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a federal information system at http://www.firstgov.gov). Related security control: IA-2.

Control Enhancements:

(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

LOW AC-14	**MOD** AC-14 (1)	**HIGH** AC-14 (1)

16 AC-15 AUTOMATED MARKING

AC-15 AUTOMATED MARKING

Control: The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

Supplemental Guidance: Automated marking refers to markings employed on external media (e.g., hardcopy documents output from the information system). The markings used in external marking are distinguished from the labels used on internal data structures described in AC-16.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** AC-15

17 AC-16 AUTOMATED LABELING

AC-16 AUTOMATED LABELING

Control: The information system appropriately labels information in storage, in process, and in transmission.

Supplemental Guidance: Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with: (i) access control requirements; (ii) special dissemination, handling, or distribution instructions; or (iii) as otherwise required to enforce information system security policy.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

18 AC-17 REMOTE ACCESS P1

AC-17 REMOTE ACCESS

Control: The organization authorizes, monitors, and controls all methods of remote access to the information system.

Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publications 800-73 and 800-78. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks. Related security control: IA-2.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

(2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

(3) The organization controls all remote accesses through a limited number of managed access control points.

(4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

LOW AC-17	**MOD** AC-17 (1) (2) (3) (4)	**HIGH** AC-17 (1) (2) (3) (4)

19 AC-18 WIRELESS ACCESS RESTRICTIONS P1

AC-18 WIRELESS ACCESS RESTRICTIONS

Control: The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system.

Supplemental Guidance: NIST Special Publications 800-48 and 800-97 provide guidance on wireless network security. NIST Special Publication 800-94 provides guidance on wireless intrusion detection and prevention.

Control Enhancements:

(1) The organization uses authentication and encryption to protect wireless access to the information system.

(2) The organization scans for unauthorized wireless access points [*Assignment: organization-defined frequency*] and takes appropriate action if such an access points are discovered.

Enhancement Supplemental Guidance: Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact information systems. The scan is not limited to only those areas within the facility containing the high-impact information systems.

LOW AC-18	**MOD** AC-18 (1)	**HIGH** AC-18 (1) (2)

20 AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES P1

AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES

Control: The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.

Supplemental Guidance: Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family. Related security controls: MP-4, MP-5.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-19	**HIGH** AC-19

21 AC-20 USE OF EXTERNAL INFORMATION SYSTEMS P1

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control: The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an

external information system.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Control Enhancements:

(1) The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system.

LOW AC-20	**MOD** AC-20 (1)	**HIGH** AC-20 (1)

22 ACCESS CONTROLS COMPLETE

This is a milestone task. Set a task to 0d duration to mark an event in your project.

24 AWARENESS AND TRAINING

This is a summary task. Use summary tasks to help organize your project into sections.

25 AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES P1

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Supplemental Guidance: The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-16 and 800-50 provide guidance on security awareness and training.
NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW AT-1	**MOD** AT-1	**HIGH** AT-1

26 AT-2 SECURITY AWARENESS P1

AT-2 SECURITY AWARENESS

Control: The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [*Assignment: organization-defined frequency, at least annually*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.

Control Enhancements: None.

LOW AT-2	**MOD** AT-2	**HIGH** AT-2

27 AT-3 SECURITY TRAINING P1

AT-3 SECURITY TRAINING

Control: The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.

Control Enhancements: None.

LOW AT-3	**MOD** AT-3	**HIGH** AT-3

28 AT-4 SECURITY TRAINING RECORDS P3

AT-4 SECURITY TRAINING RECORDS

Control: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

Supplemental Guidance: None.

Control Enhancements: None.

LOW AT-4	**MOD** AT-4	**HIGH** AT-4

29 AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS P0

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: The organization establishes and maintains contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance: To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

31 AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES P1

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Supplemental Guidance: The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW AU-1	**MOD** AU-1	**HIGH** AU-1

32 AU-2 AUDITABLE EVENTS P1

AU-2 AUDITABLE EVENTS

Control: The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].

Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after- the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined auditable events.

LOW AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (1) (2) (3)

33 AU-3 CONTENT OF AUDIT RECORDS P1

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Supplemental Guidance: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event;

(iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

(2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.

LOW AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

34 AU-4 AUDIT STORAGE CAPACITY P1

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance: The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements. Related security controls: AU-2, AU-5, AU-6, AU-7, SI-4.

Control Enhancements: None.

LOW AU-4	**MOD** AU-4	**HIGH** AU-4

35 AU-5 RESPONSE TO AUDIT PROCESSING FAILURES P1

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related security control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

LOW AU-5	**MOD** AU-5	**HIGH** AU-5 (1) (2)

36 AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING P1

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

37 AU-7 AUDIT REDUCTION AND REPORT GENERATION P2

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: The information system provides an audit reduction and report generation capability.

Supplemental Guidance: Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

Control Enhancements:

(1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.

LOW Not Selected	**MOD** AU-7 (1)	**HIGH** AU-7 (1)

38 AU-8 TIME STAMPS P1

AU-8 TIME STAMPS

Control: The information system provides time stamps for use in audit record generation.

Supplemental Guidance: Time stamps (including date and time) of audit records are generated using internal system clocks.

Control Enhancements:

(1) The organization synchronizes internal information system clocks [*Assignment: organization- defined frequency*].

LOW AU-8	**MOD** AU-8 (1)	**HIGH** AU-8 (1)

39 AU-9 PROTECTION OF AUDIT INFORMATION P1

AU-9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Control Enhancements:

(1) The information system produces audit records on hardware-enforced, write-once media.

LOW AU-9	**MOD** AU-9	**HIGH** AU-9

40 AU-10 NON-REPUDIATION P2

AU-10 NON-REPUDIATION

Control: The information system provides the capability to determine whether a given individual took a particular action.

Supplemental Guidance: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

45 CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES P1

CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	LOW	P1	Security Assessment And Authorization

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

b. Reviews and updates the current:

1. Security assessment and authorization policy [*Assignment: organization-defined frequency*]; and

2. Security assessment and authorization procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive