Multi-Factor Authentication Workbook

Activities, templates, and samples for your MFA Project

san diego county office of EDUCATION
FUTURE WITHOUT BOUNDARIES℠

Items to Consider

- **Worksheet:** Technical Considerations
- **Worksheet:** Organizational Change Management (OCM) Considerations
- **Worksheet:** Training & Support Considerations

MFA Technical Considerations

What is your ideal state? Consider the following.

Technology

1. What technology do you have?

_____

_____

2. What might you need to add?

_____

_____

3. What is your identity provider?

_____

_____

4. Which methods of authentication are preferred? *Examples: h/w or s/w token, PIN, approval app, SMS, phone, email*

_____

_____

5. What services will you protect with MFA?

_____

_____

6. What services do not use your identity provider?

_____

_____

7. Will you deploy an SSO portal with this implementation of MFA? *(Yes/No)* _____

8. How frequently should a user authenticate with MFA? Any considerations for mobile vs desktop policies?

_____

_____

People

9. Who are your users and what are their behaviors?

_____

_____

10. Onboarding – How will you onboard users? *Examples: connect via AD or manually; in waves or phases; existing staff vs new hires*

_____

_____

_____

_____

11. Are you planning to roll out MFA in phases to manage the number of employees for training and support?

- ☐ By departments/divisions
- ☐ By last name
- ☐ Start with departments that deal with sensitive information or critical business processes
- ☐ Start with IT department
- ☐ Other _____

12. How many phases will you have? _____

Process

13. How will you test? With whom? How long?

_____

_____

_____

_____

14. How tightly will you enforce vendor recommended client requirements?

_____

_____

MFA Organizational Change Management (OCM) Considerations

1. Who are your decision makers? *Please write their names and titles.*

1. _____
2. _____
3. _____
4. _____

2. Who are your bargaining unit leaders?

1. _____
2. _____
3. _____
4. _____

3. Who will you nominate to be in your governance team? Will they cover your employee base?

1. _____
2. _____
3. _____
4. _____

4. Who will you pick to be your division/department/school champions? Champions are those who have participated in the program (MFA), know what to expect, have attended training, and can help their team members with basic issues. *Example: Administrative Assistants.*

1. _____
2. _____
3. _____
4. _____

5. What do you think are the best methods of communication for different groups in your organization? *Example: Will you have different communication style for different group of users, and when will you use which style?*

	Email	Newsletter	Website	Meetings	Phone Auto Dialer	Other Method(s)	Notes
Technical							
Classified							
Teachers							
Managers							
Cabinet Members							
Casual							
Other							

6. Will you create an FAQ? Where will you house it?

- ☐ Yes. I will put it on our public website
- ☐ Yes. I will put on our intranet
- ☐ Yes. I will share it via email
- ☐ Yes. I will save it in a shared folder
- ☐ No. I will not create an FAQ

7. Will you ask departmental managers to communicate with their team regarding MFA?

- ☐ Yes. I will create an email template and share it with them.
- ☐ Yes. I will ask them to mention it during their departmental meetings.
- ☐ Yes. I will leave it up to them how to communicate with their staff.
- ☐ No. I don't think we need to do that.
- ☐ No. I will have the Champions to do this.

8. Will you have town hall style information sessions?

- ☐ Yes. I will only have one for everyone.
- ☐ Yes. I will have one for each phase.
- ☐ No. There is no need for town hall meetings.

9. Do you have all the information needed to configure MFA for your employees?
Examples: Personal phone number, or current address if you are mailing materials to your users

- ☐ Yes. I have all the information.
- ☐ Yes. But I need to confirm that information is valid.
- ☐ No. I will accept the risk of some users not getting the material sent to them.
- ☐ No. I will need to collect the information.

10. What tools do you have/use to solicit feedback?

- ☐ Microsoft Forms
- ☐ Google Forms
- ☐ Email
- ☐ Other: _____

MFA Training & Support Considerations

Training

1. Are you planning to roll out MFA in phases? How many phases will you have and how are you dividing them to manageable portions for training and support?

- ☐ By departments/divisions
- ☐ By last name
- ☐ Start with departments that deal with sensitive information or critical business processes
- ☐ Start with IT department
- ☐ Other _____

2. How will you train staff prior to go-live?

- ☐ Live meetings
- ☐ Training videos
- ☐ User guides
- ☐ Support websites

3. What job aids will you need for your users?

- ☐ How to authenticate using your mobile device
- ☐ How to authenticate with a token
- ☐ How to register a new phone number/change existing number
- ☐ How to set up authenticator app
- ☐ How to configure apps

4. How will you prepare your job aids and where will you house them?

_____

Support

5. What method(s) of support are you planning to provide?

- ☐ Phone support only – are you planning for a dedicated phone line?
- ☐ Email support only – dedicated email account?
- ☐ Ticket support – do you have a ticketing system that can handle this level of support?
- ☐ In person support – office hours
- ☐ Chat support – what tool will you be using?

6. Define your service level objectives for help desk resolution. How quickly do you need to respond to users who are having trouble with MFA?

- ☐ Within 2 hours
- ☐ Within 4 hours
- ☐ Within one day
- ☐ Within two days

7. Determine if you will have a dedicated email account and/or phone line for users to ask for help.

A. Will your users benefit from having a dedicated phone line or email for MFA support?

_____

B. Have you thought about how to communicate this new line of support?

_____

C. Do your users trust the selected email address? *Example: mfa@coe.net*

_____

8. What is your help desk capacity to provide support for Day 1 issues?

- ☐ We don't have enough staff to support our users
- ☐ We can easily support our users
- ☐ We can get help from other organizations
- ☐ We can modify our rollout groups to manageable sizes
- ☐ We can hire limited term employees from a temp agency
- ☐ We can get help from other departments and train them to support MFA

9. How will you track MFA specific issues?

- ☐ Ticketing system
- ☐ Excel sheet
- ☐ Custom database
- ☐ Other _____

10. Will you have dedicated support hours to help users with their questions or issues?

_____

11. Will you offer extended support hours? *Example: For staff working outside of normal work hours.*

- ☐ Yes. I will provide support by _____
- ☐ No. We will accept if there is a loss of productivity

12. Will you provide support for personal devices used for work purposes?

- ☐ Yes. Provide static support – user guide, FAQ, etc.
- ☐ Yes. Provide live support (in person/phone)
- ☐ Yes. Provide limited support for certain applications in specified time frame.
- ☐ No. Will not support personal user devices

13. Will you have a bypass policy?

A. What would it be? Will you use one-time pass code?

_____

B. Will you allow your users to bypass MFA if you cannot help them quickly?

_____

C. Will you allow your users to bypass MFA if they have phone issues?

Examples: lost phone, no cell coverage

_____

D. Are you willing to issue a one-time pass? If so, for how long will your one-time pass be valid?

_____

14. How will you support users with multiple email accounts? Or those who change their name?

- ☐ We will create alias for those users
- ☐ We will remove extra emails and keep one only
- ☐ We will not support users with multiple email accounts

15. If you are using a security key, there will be some users who will lose their key, break it, or misplace it. How will you deal with lost, stolen, or misplaced security keys? How are you going to support these users?

- ☐ Provide a one-time passcode
- ☐ Provide a key replacement
- ☐ Have users pay for the replacement key
- ☐ Put them on bypass

16. If you are using a security key, how will you support users who have received the wrong key for their USB port? Some users may receive USB Type A, but their device supports Type C only. They may get a new computer that no longer supports the USB key they currently have.

- ☐ Will issue a new key to them and disable the old one
- ☐ Will ask them to use SMS or app authenticator
- ☐ Will put them on bypass

17. What criteria will you use for your MFA conditional and network access control?

- ☐ Block end-of-life devices
- ☐ Don't allow authentication for apps that are no longer supported or not on an acceptable patch level
- ☐ Jailbroken devices
- ☐ Don't authenticate if users are using unsanctioned apps or devices
- ☐ Allow users to bypass MFA if they are on campus

18. Are you planning to support multiple MFA methods of authentication for each user?
Example: The security key is the primary method of authentication, but users can also use SMS or optionally phone app for authentication.

---

19. Will you need support from another COE or District?

- ☐ No
- ☐ Need help to implement
- ☐ Need help to support users
- ☐ Need help creating supporting materials
- ☐ Maybe

20. Are you willing to help another COE or Districts with their MFA?

- ☐ No
- ☐ Yes. I can help with implementation
- ☐ Yes. I can help with supporting their users
- ☐ Yes. I can help with creating supporting documents
- ☐ Maybe

Notes

Project Charter

- **Template:** Blank Project Charter Template
- **Sample:** SDCOE MFA Project Charter

Project Charter DRAFT

Project authorized by _____ on _____

I. Project Name

Project Name X	**Start Date** XX/XX/XX	**End Date** XX/XX/XX

II. Project Organization

Indicate all project team members and how frequently you will communicate with them.

Project Manager *Oversees the project work plan; reports on status; leads project team that is responsible for achieving the project objectives* • X	**Sponsor** *The top decision maker authorized to engage the project and fund it; has ultimate authority and responsibility for the project* • X
Steering Committee *Key people that assist the project manager in making decisions and moving the project forward* ☐ Weekly ☐ Bi-Weekly ☐ Monthly ☐ As Needed • X	**Stakeholders** *An individual, group, or organization that may affect or be affected by outcome of the project* ☐ Weekly ☐ Bi-Weekly ☐ Monthly ☐ As Needed • X
Project Team *Supports the project manager in performing work of the project to achieve its objectives* ☐ Weekly ☐ Bi-Weekly ☐ Monthly ☐ As Needed • X	**Others Involved** *List anyone else who will be involved and state their roles* ☐ Weekly ☐ Bi-Weekly ☐ Monthly ☐ As Needed • X

III. Project Details

Project Description

Write a brief description of this project in simple, easy-to-understand terms. What are you trying to accomplish? Why?

X

Scope

Who/how many this will impact? What is included (or not included) that can help manage the expectations?

In scope:

- X

Out of scope:

- X

Deliverables

Which products or results do you expect upon completion of the project?

- X

Goals Alignment

With which Board Goals and ITS Goals does this project align?

☐ #B1 Connect the educational experience to the world of work
☐ #B2 Provide educational opportunities and supports to SDCOE schools and school districts
☐ #B3 Become the leader and model for innovation
☐ #B4 Maximize human and operational resources to strengthen the organizational culture of SDCOE
☐ #ITS1 Maximize Customer Success
☐ #ITS2 Create Value
☐ #ITS3 Improve Division Efficiencies
☐ #ITS4 Protect•Detect•Respond

Objectives/Success Criteria

How will you know if the project was a success? List what you are trying to accomplish and the success criteria.

- X

Risks

List the things that you think could be risks to the success of the project. If possible, list the mitigation strategy for each risk.

- X

IV. Project Schedule & Milestones

Based on your needs, list either the phases and/or major milestones of the projects. Include start and end dates.

Phase/Major Milestone	Responsible (Lead)	Start Date or Month Begin	End Date or Month End
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

V. Tools

☐ Monday.com	If Yes, which board? _____ Do any new members need to be added? _____
☐ Microsoft Teams	If Yes, which team/channel will you use? _____
☐ OneDrive	If Yes, whose OneDrive, and what is the folder named? _____
☐ SharePoint Site	If Yes, which site, and what is the folder named? _____
☐ Other	

VI. Other Items to Consider

- **Project Budget:** Estimate the cost of the project.
- **Communication Plan:** Identify all critical communication channels for project stakeholders, frequency of communication, types of information to be communicated, and method of regular communication.
- **Tracking and Status Updates:** Identify the methods the project team will use to regularly update the project status including methods of tracking project progress and which organizational stakeholders receive notification of project status.
- **Training Plan/Documentation Plan**: Identify any necessary training and documentation for project stakeholders, including content, delivery method, etc.
- **Project Close Out:** Determine the final actions/steps to close out the project. Examples include sign off documentation, lessons learned meetings and documentation, surveys/evaluations, and a celebration and/or acknowledgement.

Project Charter

Project authorized by Terry Loftus on January 22, 2021

I. Project Name

Project Name	SDCOE Secure Access Project (MFA) *MFA = Multi-Factor Authentication*	**Start Date**	01/04/21	**End Date**	10/22/21

II. Project Organization

Indicate all project team members and how frequently you will communicate with them.

Project Manager
Oversees the project work plan; reports on status; leads project team that is responsible for achieving the project objectives

- **Project Manager:** Flora Pourzamani
- **Project Management Assistant:** Candace Wong

Sponsor
The top decision maker authorized to engage the project and fund it; has ultimate authority and responsibility for the project

- **Executive Sponsor:** Terry Loftus
- **Project Sponsor:** Ali Maroufi

Steering Committee
Key people that assist the project manager in making decisions and moving the project forward
☐ Weekly ☐ Bi-Weekly ☐ Monthly ☒ As Needed

- **ITS Sr. Leadership:** Terry Loftus, John Cusack, Peyri Herrera, John Vaillancourt, Beckie Benson, Tammy Carpowich

Stakeholders
An individual, group, or organization that may affect or be affected by outcome of the project
☐ Weekly ☐ Bi-Weekly ☐ Monthly ☒ As Needed

- Every permanent SDCOE employee is impacted because they will be issued a device
- Cybersecurity Team

Project Team
Supports the project manager in performing work of the project to achieve its objectives
☒ Daily ☒ Weekly ☐ Monthly ☒ As Needed

- **Core Team:** SDCOE Cybersecurity – Ali Maroufi, Ruben Sandoval, Vong Sopha
- **Graphics Lead:** Candida Bothel-Hammond
- **Support Leads:** Tyler Petro, Paola Ramos

Others Involved
List anyone else who will be involved and state their roles
☐ Weekly ☐ Bi-Weekly ☐ Monthly ☒ As Needed

- **Instructional Guidance:** Peyri Herrera
- **Graphics Dept:** Package and mail 1 USB security key + 1 job aid to each employee (in phases)
- **Communications:** Stacy Brandt
- **Media & Creative Services:** Video
- **Support:** Computer Support Services (CSS), Ops, and Cyber
- **Network:** For new MFA email account
- **Legal**
- **Duo (External)**

III. Project Details

Project Description
Write a brief description of this project in simple, easy-to-understand terms. What are you trying to accomplish? Why?

One of SDCOE's top priorities is to protect the data of our staff, students, parents/guardians, vendors, and community partners. To aid in protecting our accounts, all SDCOE employees will insert a **USB security key** into their computers or optionally use their **personal mobile phones** for multi-factor authentication (MFA) when accessing Office 365 and other secured apps. MFA is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence, or factors, in order to log in. **The goal of this project is to issue by U.S. mail one MFA security key to each permanent SDCOE employee.** The MFA security key is a small hardware device, like a USB drive. A significant component of this project is communication and organizational change management (OCM).

The USB security key is about the size of a small flash drive:

Scope

Who/how many this will impact? What is included (or not included) that can help manage the expectations?

In scope:

- All permanent computer-using SDCOE employees will be impacted (Total # = 1085)
- Secured apps: Office365, ServiceNow, Monday.com
- Employees will be issued 1 USB security key
- Employees will be given the option to authenticate using the Duo Mobile push notifications on their personal mobile phones

Out of scope:

- We will not secure Google Suite, Synergy SIS or PeopleSoft in this project
- We will secure apps only – MFA will not be used when logging in to a computer

Deliverables

Which products or results do you expect upon completion of the project?

- 1085 configured USB security keys (1 per employee), mailed via U.S. mail
- 1 multi-purpose PowerPoint presentation
- 1 'Why MFA' video
- 2 instructional videos (YubiKey, Duo Mobile)
- 3 job aids (Getting Started, YubiKey Daily Use, Duo Mobile) – the first two job aids will be mailed home with the USB security key so employees can easily follow the instructions upon receipt
- 1 opt-in form for use of personal mobile phones
- 1 dedicated phone # for MFA emergencies (aka MFA Helpline)
- Planning documents:
  - Calendar (PowerPoint)
  - Communications Plan
  - Address and Computer Type Validation Process
  - Support Procedures Plan
- Add MFA Catalog Item to ServiceNow incident

Goals Alignment

With which Board Goals and ITS Goals does this project align?

☐ #B1 Connect the educational experience to the world of work

☐ #B2 Provide educational opportunities and supports to SDCOE schools and school districts

☒ #B3 Become the leader and model for innovation

☒ #B4 Maximize human and operational resources to strengthen the organizational culture of SDCOE

☒ #ITS1 Maximize Customer Success

☒ #ITS2 Deliver Value: Applications & Systems

☐ #ITS3 Improve Division Efficiencies

☒ #ITS4 Be the Cybersecurity Solutions Leader

Objectives/Success Criteria

How will you know if the project was a success? List what you are trying to accomplish and the success criteria.

Overall goal: SDCOE employees will be secure with their password and thus our accounts and data are protected

Project success means that:

1. Every SDCOE employee (with a device) will successfully receive the USB security key and instructions via U.S. mail
2. Every SDCOE employee (with a device) will successfully use the USB security key using our instructions, which are clear and easy to follow
3. The employees' work will not be significantly interrupted (very little downtime)

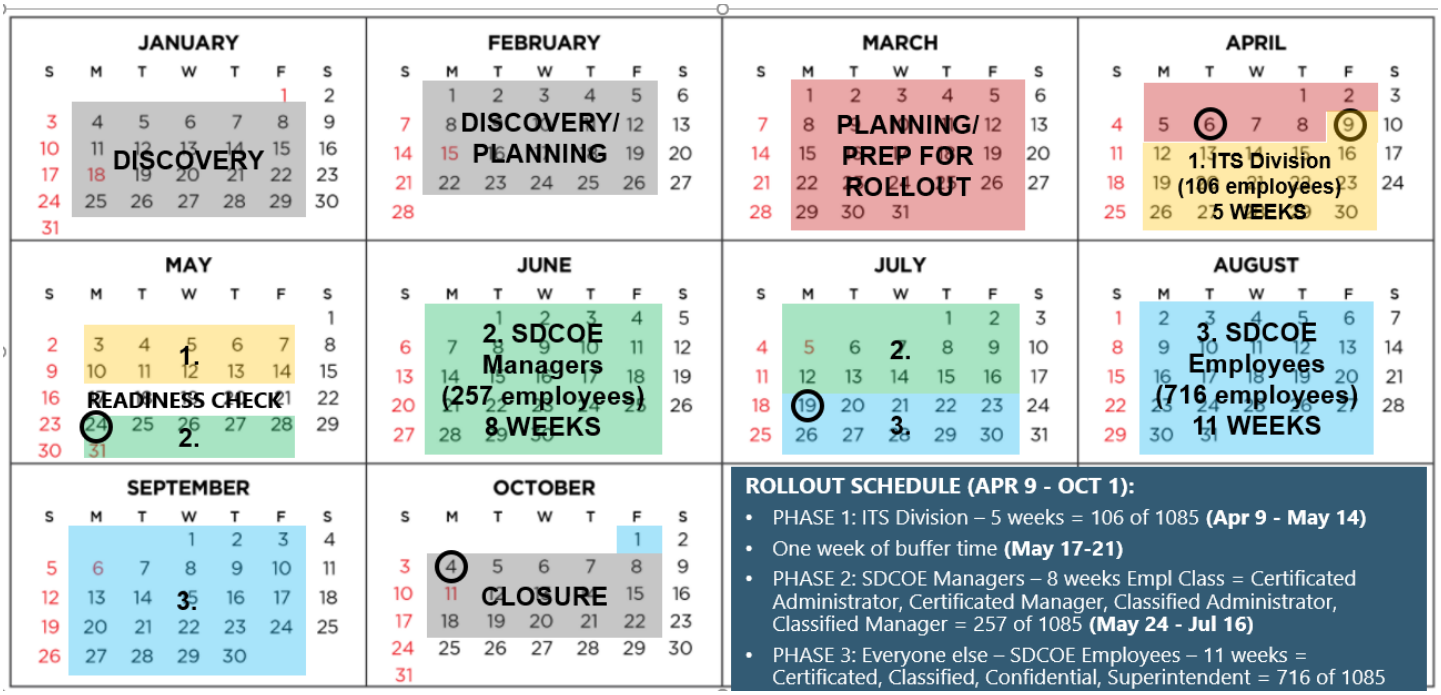
Risks

List the things that you think could be risks to the success of the project. If possible, list the mitigation strategy for each risk.

- Loss of productivity if employees need to wait too long for someone to troubleshoot – *must have support procedures in order and entire support team prepared for each Go Live*
- If they lose the USB security key or do not have a backup, they won't be able to access applications – *must have a plan for bypass, must be prepared to respond to MFA helpline (emergencies)*
- Lack of Manager support will impact adoption – *bring Managers on before Employees and ask for their help with communicating*
- Employees must follow instructions on their own to get started – *create simple, easy-to-read documents; create instructional videos*
- Bad mailing addresses in PeopleSoft – *we must ask employees to validate their addresses*
- USB security keys could get lost in the mail or not delivered

IV. Project Schedule & Milestones

Based on your needs, list either the phases and/or major milestones of the projects. Include start and end dates.



Phase/Major Milestone	Responsible (Lead)	Start Date	End Date
Discovery/Planning/Prep Phase (6 weeks) • Research different security keys, vendors, and costs • Choose a solution (security key/vendor) • Purchase the Duo licenses • Purchase the security keys • Configure Duo • Use a Teams group chat to communicate about the project • Test the security keys (PC, Mac, Chromebook) • Write instructions and troubleshooting steps • Coordinate with Graphics to mail out the security keys and job aids • Train CSS • Send communication to all ITS employees explaining the process, • Create spreadsheet that can be used to validate addresses, document receipt of security key and successful installation of the security keys	Ali/Flora	01/04/21	04/08//21

Phase/Major Milestone	Responsible (Lead)	Start Date	End Date
Phase 1 Rollout: All ITS Division - 106 employees (5 weeks) • *Send out all staff communication to let them know about the project and process and what to expect • Graphics mail out the security keys and job aids to employees • E-mail phone installation instructions to managers • Work with Admins on collecting information and documenting employees receiving the security keys and successfully installing • Collect and review feedback • Work with CSS to make sure they are trained and ready • Refine the instructions and troubleshooting if needed • Post job aid on Common Ground or in ServiceNow as a knowledgebase article • Survey all ITS staff at the end to collect feedback on the process (align the survey with the objectives)	Ali, Flora	04/09/21	05/14/21
Readiness Check (1 week) • *Terry addresses at SLT • All addresses are validated • Communication has been sent to all managers • Duo licenses have been purchased • YubiKeys have been purchases • The list of addresses and instructions have been sent to Graphics • Changes made as result of the feedbacks	Ali, Flora	05/17/21	05/21/21
Phase 2 Rollout: All SDCOE Managers – 257 managers (10 weeks) • Meet with ITS Leadership and Admin Assistants to set expectations – Admin Assistants will be asked to work with their departments to ensure that the security keys were (1) received in the mail, (2) registered/installed, and (3) able to log in successfully to Office365 and other Cloud-based services; they can use the group chat to ask questions; there will be a team to use to manage the files • *Send out all staff communication to let them know about the project and process and what to expect • Work with Admin Assistants to validate addresses • Graphics mail YubiKey security keys and instructions to all SDCOE Managers • Email instruction to install MFA on phones to all managers • Admin Assistants check in on staff and update shared spreadsheet based on timeline provided • *Conduct COMET Meeting to explain the project to managers	Ali, Flora	05/24//21	07/16/21

Phase/Major Milestone	Responsible (Lead)	Start Date	End Date
Phase 3 Rollout: All SDCOE Classified/Certificated employees – 716 employees (3 weeks) • Meet with ITS Leadership and Admin Assistants to set expectations – Admin Assistants will be asked to work with their departments to ensure that the security keys were (1) received in the mail, (2) registered/installed, and (3) able to log in successfully to Office365 and other Cloud-based services; they can use the group chat to ask questions; there will be a team to use to manage the files • *Send out all staff communication to let them know about the project and process and what to expect • Work with Admin Assistants to validate addresses • Graphics mail YubiKey security keys and instructions to all SDCOE Managers • Email instruction to install MFA on phones to all employees • Admin Assistants check in on staff and update shared spreadsheet based on timeline provided	Ali, Flora	07/19/21	10/01//21
Project Closeout (3 weeks) • Lessons Learned • Survey • Final Report • Celebration • Sponsor Sign off	Flora	10/04/21	10/22/21

V. Tools

☒ Monday.com	If Yes, which board? New **MFA Project Board** Do any new members need to be added? **Yes, all**
☒ Microsoft Teams	If Yes, which team/channel will you use? **New Team MFA**
☐ OneDrive	If Yes, whose OneDrive, and what is the folder named? _____
☐ SharePoint Site	If Yes, which site, and what is the folder named? _____
☐ Other	

VI. Other Items to Consider

- **Project Budget:** Estimate the cost of the project.
    - Duo Licenses
    - 1600 MFA security keys
    - Printing and mailing
- **Communication Plan:** Identify all critical communication channels for project stakeholders, frequency of communication, types of information to be communicated, and method of regular communication.
    - A Weekly Status Report sent via email on Fridays will be used to communicate accomplishments, in progress, what's next, and risks
    - A full communications plan will be developed
- **Tracking and Status Updates:** Identify the methods the project team will use to regularly update the project status including methods of tracking project progress and which organizational stakeholders receive notification of project status.
    - Monday.com will be used to manage all activities/tasks
    - Regularly scheduled meetings will be used to provide updates, statuses, etc.
    - A group chat for the project team only will be used for quick updates and questions
    - A group chat for the project team + Admin Assistants (per wave) will be used for quick updates and questions
- **Training Plan/Documentation Plan**: Identify any necessary training and documentation for project stakeholders, including content, delivery method, etc.
- **Project Close Out:** Determine the final actions/steps to close out the project. Examples include sign off documentation, lessons learned meetings and documentation, surveys/evaluations, and a celebration and/or acknowledgement.

Executing Your Project

- **Sample:** SDCOE MFA Project Plan in Monday.com
- **Template:** Blank Status Report
- **Sample:** SDCOE MFA Status Report (Week 2 of 31)

SDCOE SECURE ACCESS MFA PROJECT

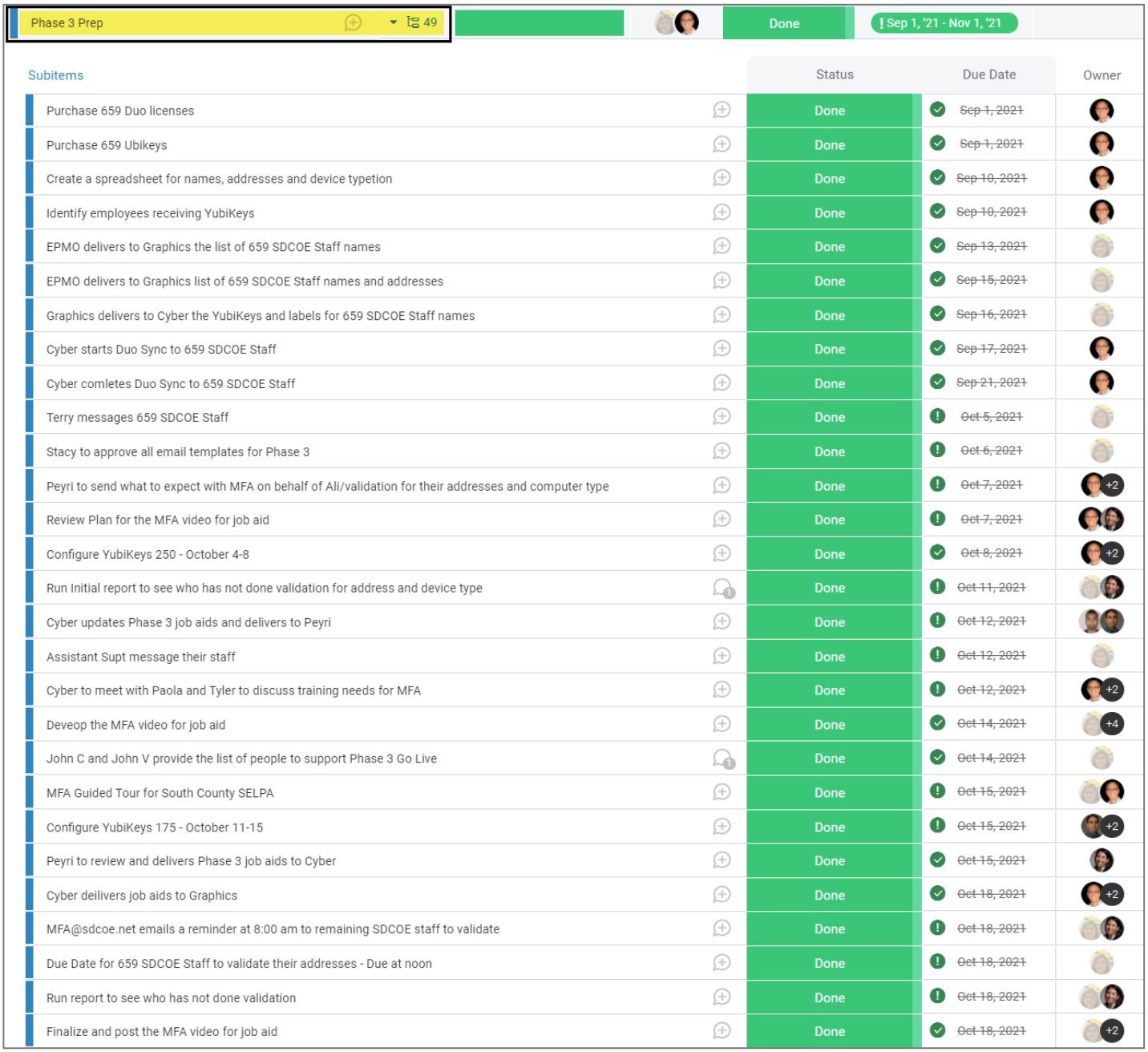
Project Plan (Monday.com)

The MFA Project was organized into phases. The project team identified the tasks associated with each phase. For example, for 'Phase 3 Prep', there were 49 tasks to be completed from September 1 thru November 1. Monday.com was used to manage the project.

Project At a Glance:

SDCOE Secure Access Project	Subitems	Subitems Status	Responsible	Status	Activity Timeline
SDCOE Secure Access Project - Overall Status				Done	Feb 15, '21 - Jan 10, '22
Planning	14			Done	Feb 19, '21 - Mar 26, '21
Testing	5		+2	Done	Jan 25, '21 - Oct 29, '21
Support Resources and Documentation	16		+2	Done	Mar 5, '21 - Apr 16, '21
Phase 1 Prep	42			Done	Mar 5, '21 - May 21, '21
Phase 1 Deployment ITS	13		+3	Done	Apr 9, '21 - Apr 21, '21
Alternate Process for 35 Managers	76			Done	Apr 23, '21 - Jul 29, '21
Phase 1B Prep - ITS Staff	17			Done	Jul 1, '21 - Aug 18, '21
Phase 1B Deployment - ITS Staff	11		+3	Done	Jul 26, '21 - Aug 26, '21
Phase 2 Prep	51			Done	Aug 2, '21 - Sep 29, '21
Phase 2 Deployment	7		+3	Done	Sep 28, '21 - Nov 5, '21
Phase 3 Prep	49			Done	Sep 1, '21 - Nov 1, '21
Phase 3 Deployment	6		+3	Done	Nov 1, '21 - Nov 2, '21
MFA Close Out	11			Done	Dec 20, '21 - Jan 21, '22

Drill Down to View ‘Phase 3 Prep’:



Phase 3 Prep	49	Done	Sep 1, '21 - Nov 1, '21

Subitems	Status	Due Date	Owner
Purchase 659 Duo licenses	Done	~~Sep 1, 2021~~	
Purchase 659 Ubikeys	Done	~~Sep 1, 2021~~	
Create a spreadsheet for names, addresses and device typetion	Done	~~Sep 10, 2021~~	
Identify employees receiving YubiKeys	Done	~~Sep 10, 2021~~	
EPMO delivers to Graphics the list of 659 SDCOE Staff names	Done	~~Sep 13, 2021~~	
EPMO delivers to Graphics list of 659 SDCOE Staff names and addresses	Done	~~Sep 15, 2021~~	
Graphics delivers to Cyber the YubiKeys and labels for 659 SDCOE Staff names	Done	~~Sep 16, 2021~~	
Cyber starts Duo Sync to 659 SDCOE Staff	Done	~~Sep 17, 2021~~	
Cyber comletes Duo Sync to 659 SDCOE Staff	Done	~~Sep 21, 2021~~	
Terry messages 659 SDCOE Staff	Done	~~Oct 5, 2021~~	
Stacy to approve all email templates for Phase 3	Done	~~Oct 6, 2021~~	
Peyri to send what to expect with MFA on behalf of Ali/validation for their addresses and computer type	Done	~~Oct 7, 2021~~	+2
Review Plan for the MFA video for job aid	Done	~~Oct 7, 2021~~	
Configure YubiKeys 250 - October 4-8	Done	~~Oct 8, 2021~~	+2
Run Initial report to see who has not done validation for address and device type	Done	~~Oct 11, 2021~~	
Cyber updates Phase 3 job aids and delivers to Peyri	Done	~~Oct 12, 2021~~	
Assistant Supt message their staff	Done	~~Oct 12, 2021~~	
Cyber to meet with Paola and Tyler to discuss training needs for MFA	Done	~~Oct 12, 2021~~	+2
Deveop the MFA video for job aid	Done	~~Oct 14, 2021~~	+4
John C and John V provide the list of people to support Phase 3 Go Live	Done	~~Oct 14, 2021~~	
MFA Guided Tour for South County SELPA	Done	~~Oct 15, 2021~~	
Configure YubiKeys 175 - October 11-15	Done	~~Oct 15, 2021~~	+2
Peyri to review and delivers Phase 3 job aids to Cyber	Done	~~Oct 15, 2021~~	
Cyber deilivers job aids to Graphics	Done	~~Oct 18, 2021~~	+2
MFA@sdcoe.net emails a reminder at 8:00 am to remaining SDCOE staff to validate	Done	~~Oct 18, 2021~~	
Due Date for 659 SDCOE Staff to validate their addresses - Due at noon	Done	~~Oct 18, 2021~~	
Run report to see who has not done validation	Done	~~Oct 18, 2021~~	
Finalize and post the MFA video for job aid	Done	~~Oct 18, 2021~~	+2

Project Name

WEEKLY STATUS REPORT

Reporting Period	Prepared By	Current Status
Month XX-XX, 2022 (Week X of X)	Project Manager Name	On Track

Project Schedule

Phase Name	Phase Name	Phase Name	Phase Name	Phase Name	Closure
In Progress Month X - Month X *X weeks*	Month X - Month X *X weeks*	Month X - Month X *X weeks*	Month X - Month X *X weeks*	Month X - Month X *X weeks*	Month X - Month X *X weeks*

Accomplishments

- Start with a verb (Example: “Completed the Project Charter”)
- X
- X

In Progress

- Start with a verb (Example: “Working on the Communications Plan”)
- X
- X

Next Steps

- Start with a verb (Example: “Schedule meeting with the Advisory Committee”)
- X
- X

Risks/Mitigation

- Example: “Short timelines to complete the project – mitigation: hold daily Standups to ensure the project is on track”
- X
- X

MFA for SDCOE Employees

WEEKLY STATUS REPORT

Reporting Period	Prepared By	Current Status
March 8-12, 2021 (Week 2 of 31)	Flora Pourzamani	On Track

Project Schedule

Planning/ Prep	Phase 1: ITS Division *106 employees*	Readiness Check	Phase 2: All SDCOE Managers *257 employees*	Phase 3: All SDCOE Employees *716 employees*	Closure
In Progress Mar 1-26 4 weeks	Mar 29 - Apr 30 5 weeks	May 3-7 1 week	May 10 - Jun 30 8 weeks	Jul 1 - Sep 10 11 weeks	Sep 13-30 3 weeks

Accomplishments

- Finalized the project charter
- Completed the rollout plan
- Obtained the mailing addresses for ITS employees
- Completed the draft of the job aid to be sent to the employees
- Completed the drafts of the job aids to be posted on Common Ground
- Identified the customer teams and support phone number (858-292-3700 / 858-CYBER-00)
- Tested Duo SMS text message, Mobile and YubiKey enrollment
- Tested Office 365 login with Duo push and YubiKey

In Progress

- Purchasing Duo licenses
- Purchasing MFA YubiKeys
- Graphics is creating the proof of the sticker to be affixed to the YubiKeys
- Finalizing the job aids
- Training Computer Support Services (CSS) for MFA customer troubleshooting
- Getting a new page set up on Common Ground
- Determining how SSO will work

Next Steps

- Email to all ITS employees a welcome message to communicate the project and expectations
- Validate ITS employees' mailing addresses and device types (PC or Mac)
- Complete the job aid to be mailed to the employees
- Design the new MFA page on Common Ground and post the job aids
- Configure Production Duo Admin Portal
- Create administrative group for CSS
- Connect Azure to Duo

- Add Phase 1 users in Duo
- Configure and test Office365 to work in Duo
- Configure and test ServiceNow to work in Duo
- Configure and test Monday.com to work in Duo

Risks

- A delay in the delivery of Duo and/or YubiKeys will put the Phase 1 rollout for ITS (March 29) at risk – To mitigate, we will highly track the order delivery

Communications Plan

- **Sample:** SDCOE MFA Communications Plan
- **Sample:** SDCOE Initial Email
- **Sample:** SDCOE Division Lead Email
- **Sample:** SDCOE What to Expect Email
- **Sample:** SDCOE Go Live Email
- **Sample:** SDCOE MFA Presentation

SDCOE SECURE ACCESS MFA PROJECT

Communications Plan

For Phase 3

Date	Audience	Message	Delivery Method	Work with Comms Dept	Owner (Sender)
10/05/21	667 SDCOE Staff with copy to 260 SDCOE Managers	Initial MFA message	Email	Yes	Terry
10/07/21	667 SDCOE Staff	Validating addresses and computer type, How will MFA work	Email	Yes	Peyri/Flora
10/12/21	Staff in their division	Support MFA and validate addresses and computer type	Email	Yes	Assistant Superintendents
10/18/21 at 7:30	Remaining SDCOE Staff who have not validated	Reminder to validate addresses and computer type	Email	No	Peyri/Flora
10/19/21	667 SDCOE Staff	What to do prior to Nov 2 and on/after Nov 2	Email	Yes	Ali/Flora
10/20/21	667 SDCOE Staff	MFA Guided Tour #1	Teams	N/A	Ali
10/21/21	667 SDCOE Staff	MFA Guided Tour #2	Teams	N/A	Ali
10/27/21	667 SDCOE Staff	Packets have been sent home and what to do	Email	Yes	Ali
11/01/21	667 SDCOE Staff	What to expect on Go Live What to do if you have not received your packet or the correct YubiKey	Email	Yes	Ali

Date	Audience	Message	Delivery Method	Work with Comms Dept	Owner (Sender)
11/01/21 DAY BEFORE GO LIVE	260 SDCOE Managers	Your SDCOE Staff are going live with MFA	Email	Yes	Ali
11/02/21 GO LIVE	667 SDCOE Staff	Go Live message and what to do	Email	Yes	Ali
11/16/21	667 SDCOE Staff	SDCOE Security Access Survey	Email	Yes	Ali

Sample Initial Email

To: Approximately 667 SDCOE Staff (Phase 3)
From: Asst Supt ITS
Subject: SDCOE Secure Access - All Staff
Date to Send: Tuesday, 10/5/21

Dear Colleagues,

As you are aware, one of SDCOE's top priorities is to protect the data of our staff members (like you), students, parents/guardians and our vendors and community partners. To further secure our organization and our collective data, the Integrated Technology Services division has built a strategy to implement multi-factor authentication (MFA) for SDCOE. MFA is a proven approach in drastically reducing automated cybersecurity attacks, with research from both Microsoft and Google noting that MFA blocks 99% of all automated account takeover attacks. Watch this video to learn more about MFA.

You are probably familiar with MFA already. For example, when you log in to your online banking account, it is highly likely that you first must enter a PIN that is sent to you via text message in order to access your account. At SDCOE, our goal is that all employees will use MFA when accessing secured applications, including Office 365, Common Ground, and ServiceNow. This initiative is called SDCOE Secure Access. Instead of a PIN, we will be issuing you a USB security key that you simply insert into your computer, similar to a flash drive. **For all SDCOE staff members, MFA will begin on Nov. 2.**

Here's what you can expect:

- **Starting Oct. 7,** please look for an email from MFA@sdcoe.net with a link to a Microsoft Form to verify/correct your mailing address and the type of SDCOE-issued computer you use (PC or Mac). *It is very important that you participate in this validation process, due by* ***noon on Oct. 18****.*
- On **Oct. 20** and **Oct. 21**, please join us at an MFA Guided Tour, hosted by our project team. We will walk you through what to expect on Nov. 2 and answer any questions you might have about MFA. It is important that you join one of these meetings.
- On **Oct. 26**, we will mail home your security key and instructions. When you receive your packet in the mail, please follow the instructions provided. The packet includes:
    - 1 USB security key
    - *Getting Started with Your New Security Key* (one page instructions)
    - *Security Key Daily Use Directions*, which includes how to get help (four pages)
- On **Nov. 2,** all SDCOE employees will use their security keys for MFA
    - Plan to use your security key every time you access secured applications on your computer. You will need it to access Office 365 apps (both web and desktop versions) and ServiceNow as it will ask you to authenticate with your security key. Your instructions will help to know which apps will require you to use your security key and how often you will use it.
    - OPTIONAL: Some employees may opt to use their personal mobile phone to access apps like Teams, Outlook, OneDrive, and so on for work purposes. You may optionally set up your personal mobile phone as a secondary method to use for MFA. Please see *MFA for Your Personal Mobile Phone (OPTIONAL)* for more information.

We have already successfully implemented SDCOE Secure Access for the entire ITS division and have been using MFA daily since June. Staff members using it have said they find MFA easy to use. On Sept. 29, we successfully implemented SDCOE Secure Access for all SDCOE managers.

If you have any questions, please contact [Name], [Title].

Sincerely,

Sample Division Leads Email

To: Employees in your division (including Managers so they are aware)
From: Division/Department Lead
Subject: Getting Ready for SDCOE Secure Access
Date to Send: Please send between October 12-14

Dear Team,

As you may have read in the **Oct. 5** email from Assistant Superintendent Terry Loftus, SDCOE is implementing an important multi-factor authentication (MFA) initiative, known as SDCOE Secure Access, to help ensure our sensitive data is safe. MFA can drastically reduce automated cybersecurity attacks that put our data and systems at risk. Please watch this two-minute video to learn more: SDCOE Secure Access "Why MFA" Video

On Oct. 7, you should have received an email message from MFA@sdcoe.net with a link to a form to verify your mailing address and the type of computer you use (PC or Mac). It is very important that you click the link in the email and submit your response by **noon on Oct. 18**.

The SDCOE Secure Access project team is providing us two opportunities to learn more about MFA and what to expect. Please plan to attend a session on either **Oct. 20** or **Oct. 21**, both offered in Microsoft Teams.

- **MFA Guided Tour #1** – Wed., Oct. 20 from 10:00-10:45 a.m.
  Click here to join the meeting
- **MFA Guided Tour #2** – Thur., Oct. 21 from 1:30-2:15 p.m.
  Click here to join the meeting

The Integrated Technology Service division and managers across the organization are already using the system. **MFA will be rolled out to all employees starting Nov. 2.**

I wanted to make sure you were aware that this initiative is coming and let you know how important it is for our organization. If you have any questions about it, you can reach out to Flora Pourzamani at fpourzam@sdcoe.net.

[Insert closing and email signature]

Sample What to Expect Email

To: Approximately 667 SDCOE Staff (Phase 3)
From: MFA@sdcoe.net (sent by Project Lead from MFA account)
Subject: What to expect for MFA on Nov. 2
Date to Send: Tuesday, 10/19/21

Dear SDCOE Staff,

Multi-Factor Authentication (MFA) is right around the corner! All SDCOE staff will receive 1 USB security key and instructions and MFA will begin on **Nov. 2 at 7:30 a.m.**

Q: How do you suggest I get ready for MFA?

It is important that you feel confident and ready for Nov. 2! Please watch this 90-second video that shows how you will insert your USB security key into your computer starting Nov. 2.

We strongly recommend that you join us this week at an MFA Guided Tour in Teams to see how you will use your USB security key. There will be time for questions and answers. These sessions will be recorded.

- ***MFA Guided Tour #1*** – Wed., Oct. 20 from 10:00-10:45 a.m. Click here to join the meeting
- ***MFA Guided Tour #2*** – Thur., Oct. 21 from 1:30-2:15 p.m. Click here to join the meeting

Q: When will I receive my USB security key?

Starting Oct. 26, through U.S. Mail we will send to your mailing address on file 1 USB Security Key and instructions to use starting Nov. 2. Please check your mail from Oct. 27 thru Nov. 1. If you do not receive your package in the mail by Nov.1, please contact Flora Pourzamani (fpourzam@sdcoe.net).

Q: Is there an option to use my personal mobile phone for MFA?

Yes, and it is completely optional. If you would like to optionally use your personal mobile phone to access apps associated with your SDCOE account, you can set up your personal mobile phone as a secondary method to use for MFA using the Duo Mobile app. All details and instructions are in this job aid. Please note that a mobile app consent form is needed if you pursue this option. The first day that you can submit the consent form and set up your personal mobile phone for MFA is **Nov. 2** (same as your USB security key).

Q: What should I expect starting Nov. 2?

1. **Restart your computer.** On Nov. 2 at or after 7:30 a.m., please restart your computer before starting your daily work.
2. **Have the materials handy.** Take out the package that was mailed home and refer to the security key instructions. If you will be optionally using Duo Mobile push notifications, please see the mobile phone instructions.
3. **Be ready to authenticate (USB security key or Duo Mobile app).** When you see a Duo Security window pop up on your screen, follow the provided instructions to use your USB security key (or, optionally, Duo Mobile on your personal mobile phone). If you are using your USB security key, insert it into your computer, docking station, or USB hub with the “y” (gold contact) facing up. On the Duo Security prompt on your screen, click “Enter a Passcode”, make sure your cursor is in the text box, then touch the “y” on your security key.

4. **We are here to help!** Our support team is here to help you if you need any guidance along the way. If you need assistance with MFA, please submit a support ticket at https://service.sdcoe.net > Report an Issue > I am having trouble with SDCOE Secure Access. If you have an emergency related to MFA, please call (858) 292-3700 from 7:30 a.m. through midnight (weekdays).

Thank you for taking part in helping protect student and employee data and keeping our information systems more secure. For more details, please go to *Common Ground* > *Documents* > *For New Hires* > SDCOE Secure Access.

Sincerely,

Sample Go Live Email

To: Approximately 667 SDCOE Staff (Phase 3)
From: Project Lead
Subject: SDCOE Secure Access Starts This Morning
Date to Send: 11/2/21

Dear SDCOE Colleagues,

It is launch Day for SDCOE Secure Access multi-factor authentication (MFA), which will start at 7:30 a.m.

What to expect today:
If you plan on using Duo Mobile app, please make sure you have completed the Mobile app consent form. Go to *https://service.sdcoe.net* > *Request Something* > *Accounts & Secure Access* > *SDCOE Secure Access (MFA) for Personal Mobile Phone*. Read the form, check the appropriate boxes, and click submit.

Please restart your computer before starting your daily work today. When prompted, use your security key or Duo Mobile app to authenticate.

How to get help:
You can find resources to help you get started on *Common Ground*. If you cannot find what you are looking for, contact Cybersecurity team at securinginfo@sdcoe.net**.**

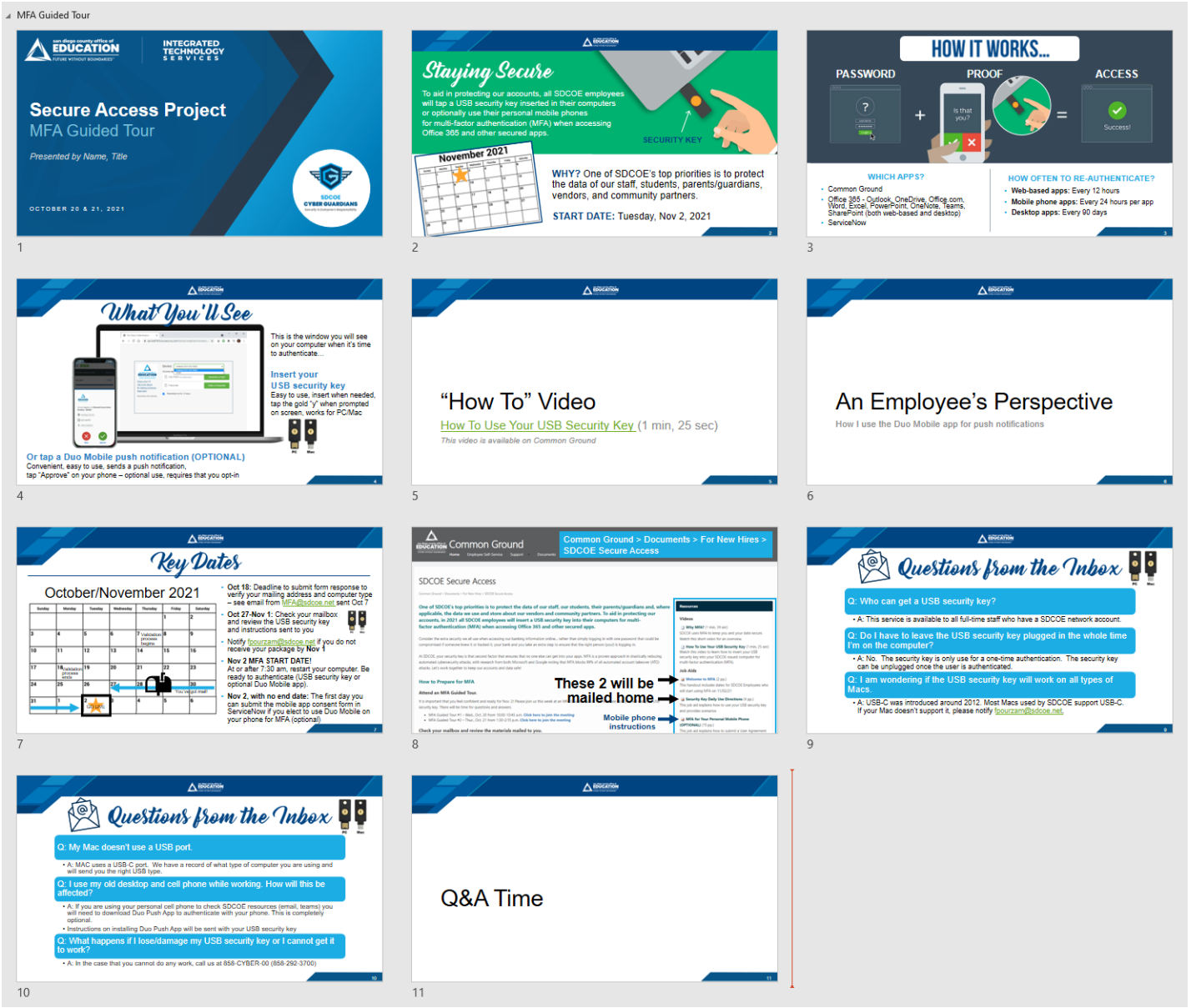
How to report issues:
- If you need assistance, please submit a support ticket at https://service.sdcoe.net by clicking “Report an Issue” and “I am having trouble with SDCOE Secure Access.”
- If you have an urgent issue, call 858-292-3700 from 7:30 a.m. to midnight on weekdays. Outside these hours, leave a message and someone will get back to you as soon as possible.

If you have any questions, please contact [Name], [Title].

Sincerely,

SDCOE SECURE ACCESS MFA PROJECT

MFA Presentation



- **Slide 1:** Welcome and Introductions
- **Slide 2:** Present 'the why' and the timeline
- **Slide 3:** How it Works
- **Slide 4:** What You'll See
- **Slide 5:** Play video
- **Slide 6:** Provide a testimonial from an employee who has been using MFA
- **Slide 7:** Key Dates
- **Slide 8:** Where to find job aids, resources, and more information
- **Slides 9-10:** FAQs
- **Slide 11:** Time for Q&A

Closure Items

- **Template:** Lessons Learned Worksheet
- **Sample:** SDCOE MFA Survey
- **Sample:** SDCOE MFA Project Final Report
- **Sample:** SDCOE MFA Project Celebration

PROJECT NAME

Lessons Learned Worksheet

Team Name

Q1: What worked well?

- X
- X
- X

Q2: Where can we improve?

- X
- X
- X

Q3: What are you most proud of as a result of this project?

- X
- X
- X

SDCOE Secure Access Survey Questions

Survey Name:

SDCOE Secure Access Survey for SDCOE Staff

Opening Text:

PURPOSE: The project sponsor and steering committee for the SDCOE Secure Access Project are interested in hearing your feedback about the deployment of multi-factor authentication (MFA) on November 2 and your experience with MFA since the Go Live. Your responses and comments are very valuable and will help to improve the future deployments. Your honest responses will be most helpful.

SURVEY TIMEFRAME: Wednesday, November 10 - Friday, November 19, 2021 at 5 pm

CONTACT: Please contact [First Last] with any questions about this survey.

Questions:

* = Required

- ***Q1. Which method(s) of authentication do you use? *(Response required for each line below using Likert scale format)***
  Description line: Primary = Your main method
  Alternate = Another method you have used
  N/A = You do not use this method

	Primary	Alternate	N/A
A. Security Key (YubiKey)			
B. Duo Mobile app on personal mobile phone			
C. SMS text messages sent to personal mobile phone			

- ***Q2. To what extent do you agree that authentication is simple for each of these methods? *(Response required for each line below using Likert scale format)***
  Description line: N/A = You do not use this method

	1 - Strongly Disagree	2 - Disagree	3 - Agree	4 - Strongly Agree	N/A
A. Security Key (YubiKey)					
B. Duo Mobile app on personal mobile phone					
C. SMS text messages sent to personal mobile phone					

- **Q3. OPTIONAL: For Question 2, please explain why you selected those values. *(Open-ended, text box)***

- ***Q4. I understand the importance of using SDCOE Secure Access authentication. *(Multiple choice)***
  - 1 - Strongly Disagree
  - 2 - Disagree
  - 3 - Agree
  - 4 - Strongly Agree

- ***Q5. The job aids provided were clear and easy to follow. *(Multiple choice)***
  Description line: Please go to Common Ground > Documents > For New Hires > SDCOE Secure Access page to find the job aids titled "Security Key Daily Use Directions" and "MFA for Your Personal Mobile Phone (OPTIONAL)".
  - 1 - Strongly Disagree
  - 2 - Disagree
  - 3 - Agree
  - 4 - Strongly Agree
  - N/A - I did not refer to any job aids

- **Q6. OPTIONAL: For Question 5, please provide feedback or suggestions on how the job aids can be improved. *(Open-ended, text box)***

- ***Q7. Which methods of help or support have you used? Please select all that apply. *(Multiple choice, multiple answers)***
  - Referred to the printed job aid(s) mailed home
  - Referred to the electronic job aid(s) available on Common Ground
  - Submitted a support ticket through ServiceNow
  - Called the MFA Helpline at 858-CYBER-00 for emergency support
  - Asked a colleague
  - No help/support needed so far
  - Other _____

- ***Q8. My questions and issues about MFA (SDCOE Secure Access) were answered in a timely manner. *(Multiple choice)***
  - 1 - Strongly Disagree
  - 2 - Disagree
  - 3 - Agree
  - 4 - Strongly Agree
  - N/A - I did not submit/ask a question

- **Q9. OPTIONAL: For Question 8, please tell us about your experience. *(Open-ended, text box)***

- **Q10: OPTIONAL: Do you have any suggestions to help us improve our process for the future deployments of MFA to the rest of the organization? *(Open-ended, text box)***

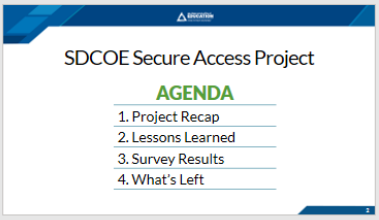
Thank You Message (Upon Submit):

Thank you for providing feedback about your experience with multi-factor authentication (MFA). All responses will be reviewed by our SDCOE Secure Access Project Team to help improve future deployments. If you have any questions about this survey, please contact First Last, Job Title, Department.

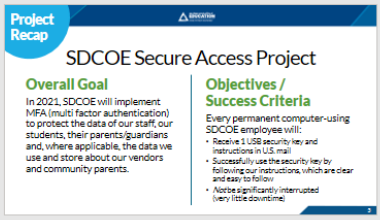
MFA Final Report

Final Report

1

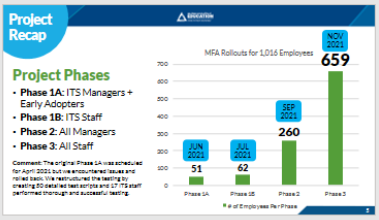


2

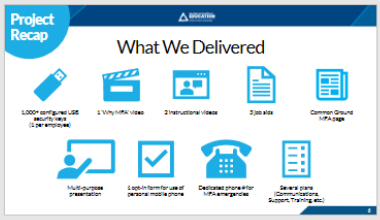


3

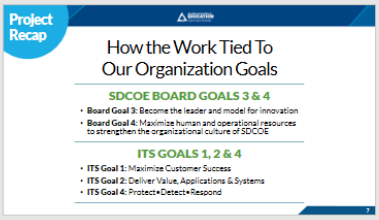
4



5

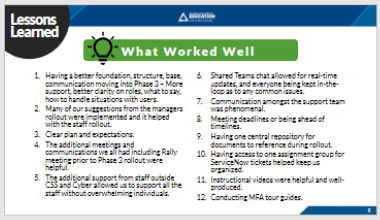


6

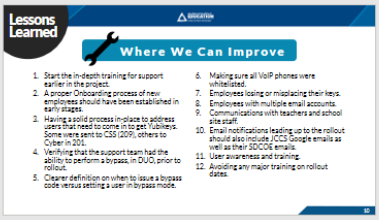


7

8

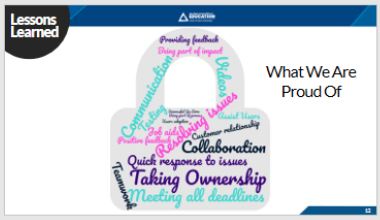


9

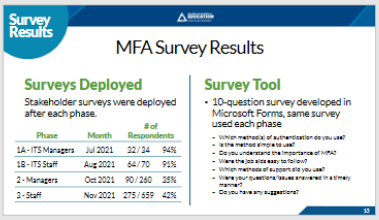


10

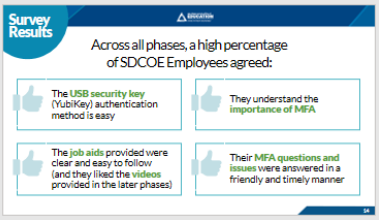
11



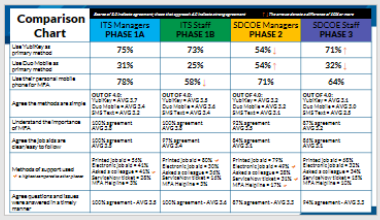
12



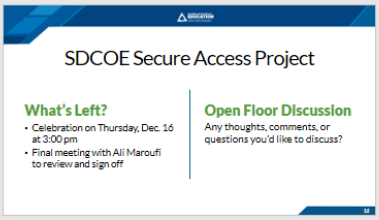
13



14



15



16

Audience: Presented to Project Sponsor, Steering Committee, and any other pertinent stakeholders

Contents of Final Report:

- **Slide 1-2:** Welcome and Agenda
- **Slides 3-7:** Project Recap
  Goal, Objectives/Success Criteria, Who was involved, Phases, Deliverables, Tying to Organization Goals
- **Slides 8-12:** Lessons Learned
  What worked well, Where we can improve, What we are proud of
- **Slide 13-15:** Survey Results
  Information about surveys deployed, survey tool, summary of feedback, comparison chart across phases

Comparison Chart	*Scores of 3.0 indicate agreement; those that approach 4.0 indicate strong agreement*		*↑↓ The arrows denote a difference of 10% or more*	
	ITS Managers **PHASE 1A**	ITS Staff **PHASE 1B**	SDCOE Managers **PHASE 2**	SDCOE Staff **PHASE 3**
Use YubiKey as primary method	**75%**	**73%**	**54%** ↓	**71%** ↑
Use Duo Mobile as primary method	**31%**	**25%**	**54%** ↑	**32%** ↓
Use their personal mobile phone for MFA	**78%**	**58%** ↓	**71%**	**64%**
Agree the methods are simple	**OUT OF 4.0:** YubiKey = **AVG 3.7** Duo Mobile = **AVG 3.4** SMS Text = **AVG 3.2**	**OUT OF 4.0:** YubiKey = **AVG 3.5** Duo Mobile = **AVG 3.6** SMS Text = **AVG 3.4**	**OUT OF 4.0:** YubiKey = **AVG 3.2** Duo Mobile = **AVG 3.2** SMS Text = **AVG 3.1**	**OUT OF 4.0:** YubiKey = **AVG 3.1** Duo Mobile = **AVG 3.0** SMS Text = **AVG 2.5**
Understand the importance of MFA	100% agreement **AVG 3.8**	100% agreement **AVG 3.8**	92% agreement **AVG 3.5**	87% agreement **AVG 3.2**
Agree the job aids are clear/easy to follow	100% agreement **AVG 3.5**	97% agreement **AVG 3.4**	84% agreement **AVG 3.1**	86% agreement **AVG 3.1**
Methods of support used ✔ = *highest compared to other phases*	Printed job aid = 56% Electronic job aid = 41% Asked a colleague = 41% ✔ ServiceNow ticket = 28% MFA Helpline = 3%	Printed job aid = 80% ✔ Electronic job aid = 30% Asked a colleague = 36% ServiceNow ticket = 16% MFA Helpline = 3%	Printed job aid = 79% Electronic job aid = 49% ✔ Asked a colleague = 28% ServiceNow ticket = 31% ✔ MFA Helpline = 17% ✔	Printed job aid = 68% Electronic job aid = 32% Asked a colleague = 34% ServiceNow ticket = 15% MFA Helpline = 10%
Agree questions and issues were answered in a timely manner	100% agreement - **AVG 3.5**	100% agreement - **AVG 3.6**	87% agreement - **AVG 3.3**	94% agreement - **AVG 3.3**

- **Slide 16:** What's Left / Discussion

MFA Project Celebration

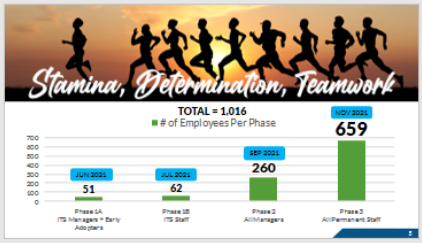
MFA Project Celebration

1

2

3

4

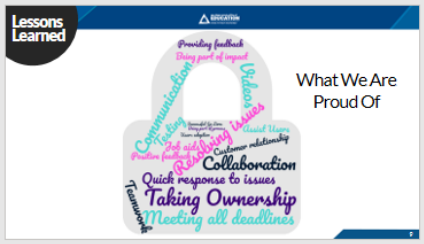


5

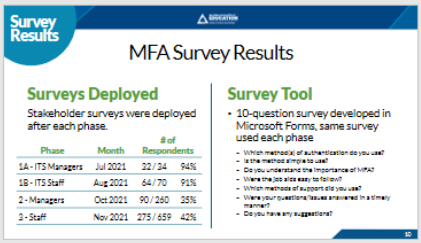
6

7

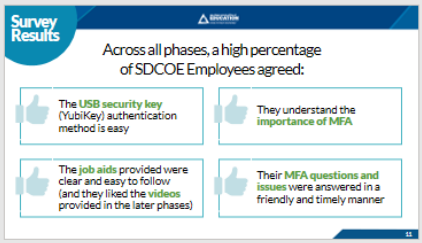
8



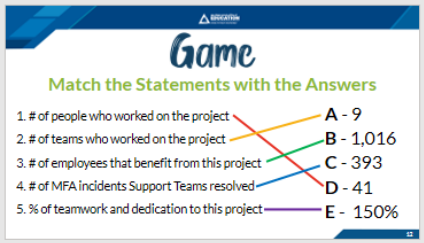
9



10



11



12

13

Audience: For the entire project team (anyone who worked on the rollout)

Theme: Running, Marathon

Fun elements included: Graphics related to running, pick a gif, matching game, played Chariots of Fire song

Agenda:

- **Slide 1:** Welcome and Agenda
- **Slides 2-8:** Project Recap
  Goal, Objectives/Success Criteria, Who was involved, Phases, Deliverables, Tying to Organization Goals
- **Slides 9:** What we are proud of (from the Lessons Learned)
- **Slide 10-11:** Survey Results
  Information about surveys deployed, survey tool, summary of feedback
- **Activity:** Select a gif that depicts how you feel now that the project is over
- **Words from Project Sponsor**
- **Slide 12:** Matching Game (interactive)
- **Slide 13:** Thank You / Open Floor / Dismissal