



WELCOME TO THE MAY 3, 2023 ISOAG MEETING



AGENDA

Welcome/Opening Remarks Mike Watson/VITA

Compliance Plus Component of KB4 Breon Worthy

Updates to International Travel Policy Jacquelyn Esters/VITA

KB4 Update Tina Gaines/VITA

ASAP KnowBe4 Thomas Claiborne

Update SEC530 Chandos Carrow

Upcoming Events Tina Gaines/VITA

Adjourn

KnowBe4
Human error. Conquered.



Breon Worthy

Enterprise Customer Success Manager

5 years of service

My CSM Role Includes:

- Implementation of the product - Helping to create the first Phishing/Training Campaign to employees within 90 days.
- Assist with management and upkeep - Continuing to provide support post-onboarding to ensure your organization is getting a return on its investment.
- Updates on the latest products and feature changes - As we roll out fresh training content, new features, product updates and more, I keep will keep you updated.
- Best Practices - Working with many large organizations from various industries I help explore proven methods that will help your organization build the strongest human firewall possible.
- Purchases and Add-ons

KnowBe4
Human error. Conquered.

KnowBe4 Resources

Point of Contact Tina Gaines

Tina.Gaines@vita.virginia.gov
804.510.7068

KnowBe4 Technical Support:

The blue question mark in the top right hand corner of your console (contact support)

KnowBe4 Knowledgebase:

Same question mark at the top right hand corner. Here you will find videos, FAQs and step by step guides for all things KnowBe4



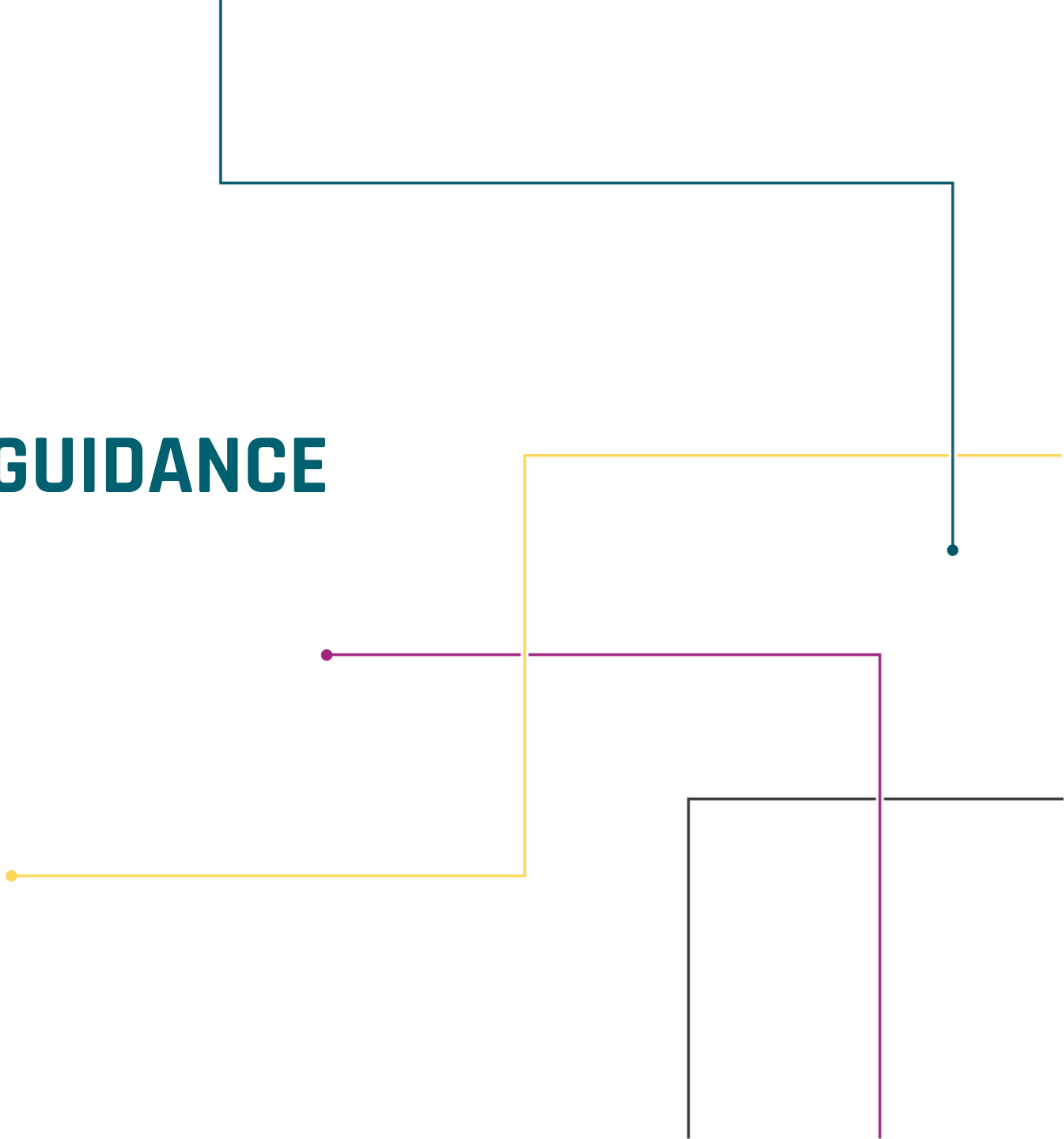
INTERNATIONAL TRAVEL GUIDANCE UPDATES

JACQUELYN ESTERS

Security Architect

ISOAG

MAY 2023



AGENDA

- WHAT'S CHANGED
- PURPOSE
- STEPS NEEDED
- COLOR CODED MAP
- KSE FORM
- QUESTIONS



1. Instead of requiring a security exception first, a KSE work request form has now been implemented

<https://vccc.vita.virginia.gov/vita?id=search&spa=1&q=international%20travel>

All results for "international travel"



International Travel

Use this form when preparing for international travel and access to Com required.



ation technology (IT) resources may be



International Travel

This is to provide guidance for Agency ISOs that have users traveling abroad; w Agency ISOs need to review the Travel Advisories (use URL below)

Article: KB0018147 · Published: 28d ago



to access Commonwealth IT resources:

PURPOSE

- This control is to provide guidance for agency ISOs that have users traveling abroad; who may be required to access Commonwealth IT resources



STEPS NEEDED

- When preparing to travel abroad, the submitted KSE request will be sent to the agency Information Security Officer (ISO) for approval. Before approving, the agency ISO will validate all security requirements have been met in accordance with the SEC501 CM-2-COV-4/ International Travel knowledge base article (KBA)



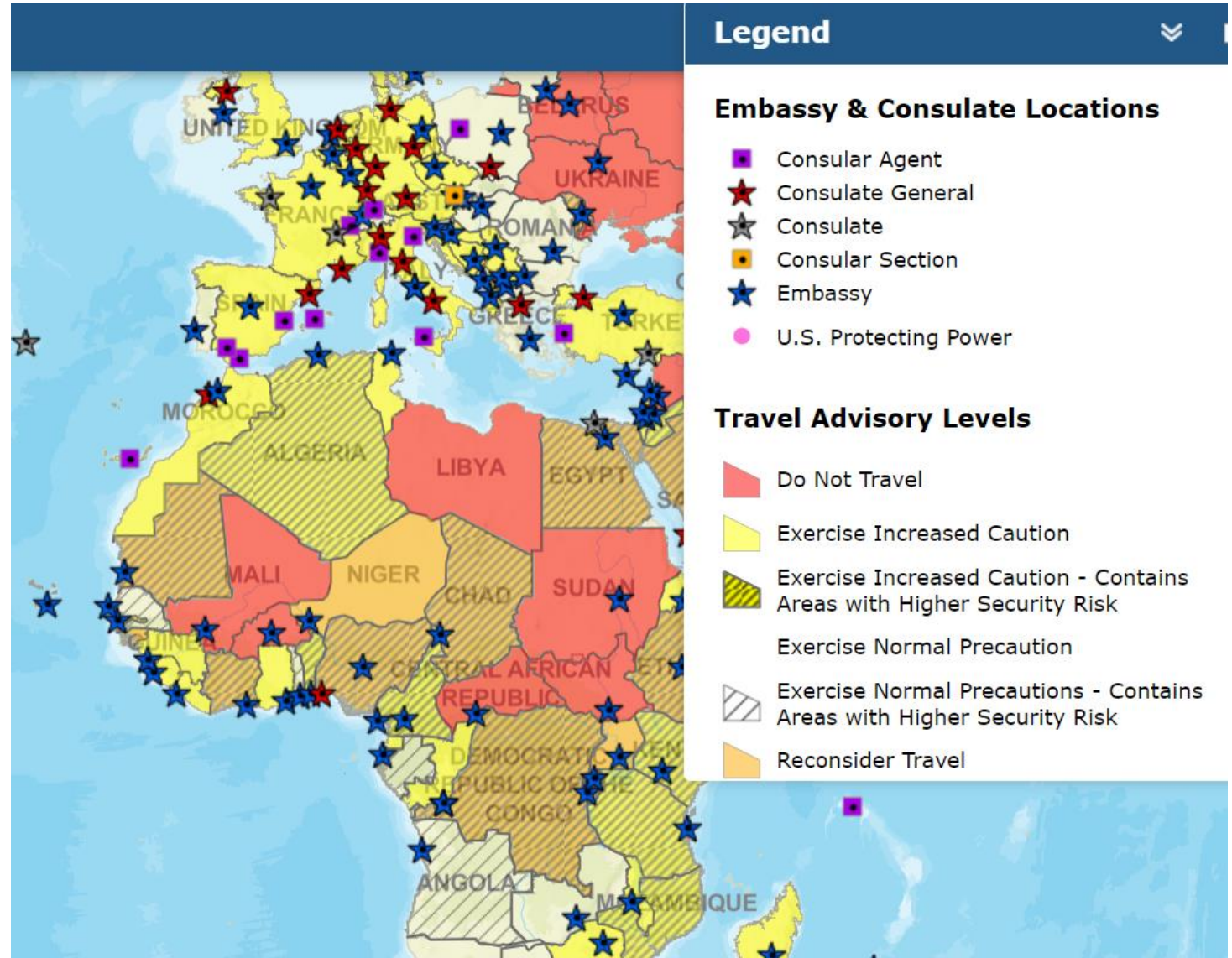
PLEASE NOTE

- Before submitting request, the first step is to review the travel advisories list when planning any trip abroad, check the Travel Advisories for your intended destination. You can see the world at a glance on the color-coded map.
- Note that conditions can change rapidly in a country at any time. To receive updated Travel Advisories and Alerts, choose the method that works best for you at travel.state.gov/stayingconnected
- **If the location is rated a 3 or 4 the user cannot bring a COV device with them on their travel.** Some countries have regions that are higher rated than the entire country, please ensure to review the entire Travel Advisory making sure the region of the user's travel is within the describe parameters.

<https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/>

COLOR CODED MAP

- Color coded map of travel designations and the advisory level
- <https://travelmaps.state.gov/TSGMap/>



STEPS NEEDED (CONT)

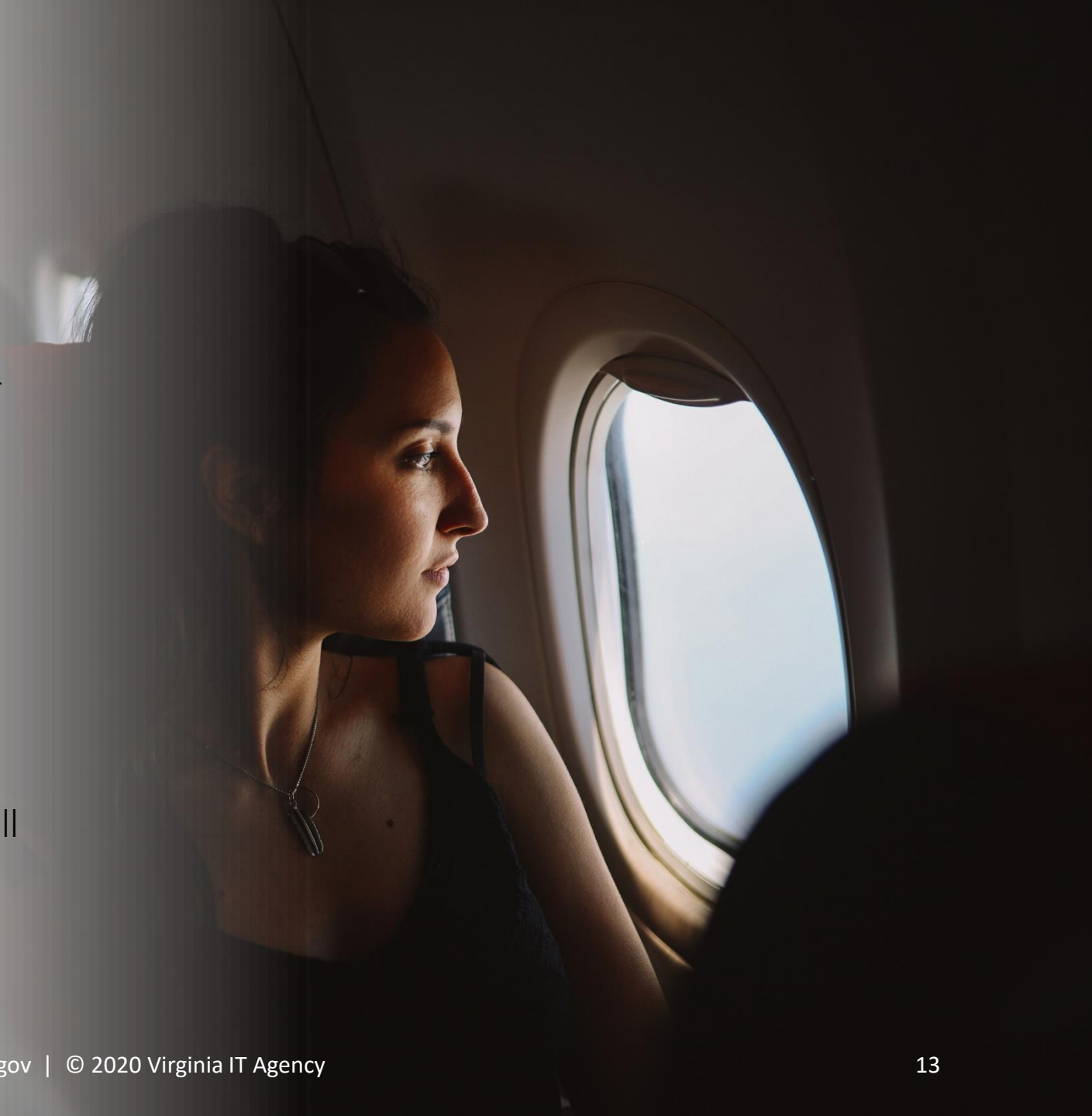
- Once the ISO approves the KSE form, a notification will be sent to the Security Operations Center (SOC) to expect international traffic from the specified user, location, device and dates. If international traffic is detected outside of these parameters, it will be blocked and the account disabled.



STEPS NEEDED (CONT)

- If the user traveling abroad needs a computer or MiFi, a loaner device should be utilized. The loaner device is issued to prevent the exposure of proprietary, sensitive, or classified information through either data theft or data leakage while abroad.
- If the individual requesting to bring a COV device with them while traveling internationally requests to bring their normally assigned device and not a loaner a security exception must be filed and approved by CSRM before they travel. If this is not done their access while traveling internationally will be disabled until they return without any warning.

Note: All devices brought out of the country will be wiped and reinstalled with zero data carry over before being allowed back on the COV network.



KSE FORM

Use this form when preparing for international travel and access to Commonwealth information technology (IT) resources may be required.

Jacquelyn Esters x

Email: Jacquelyn.Esters@vita.virginia.gov Agency: VITA - 0136

* User traveling abroad

Email address: Alias:

* Departure date: YYYY-MM-DD * Return date: YYYY-MM-DD

* Travel location(s) ?
Please provide all cities and countries of any travel destinations with tentative dates for each. x

* Will a COV device be taken abroad?
Yes

* Asset tag - Normal COV device

* Asset tag - Loaner COV device

* Location of loaner device upon return ?
Provide the address of where the loaner device will be located after returning from international travel. x

City: Zip:

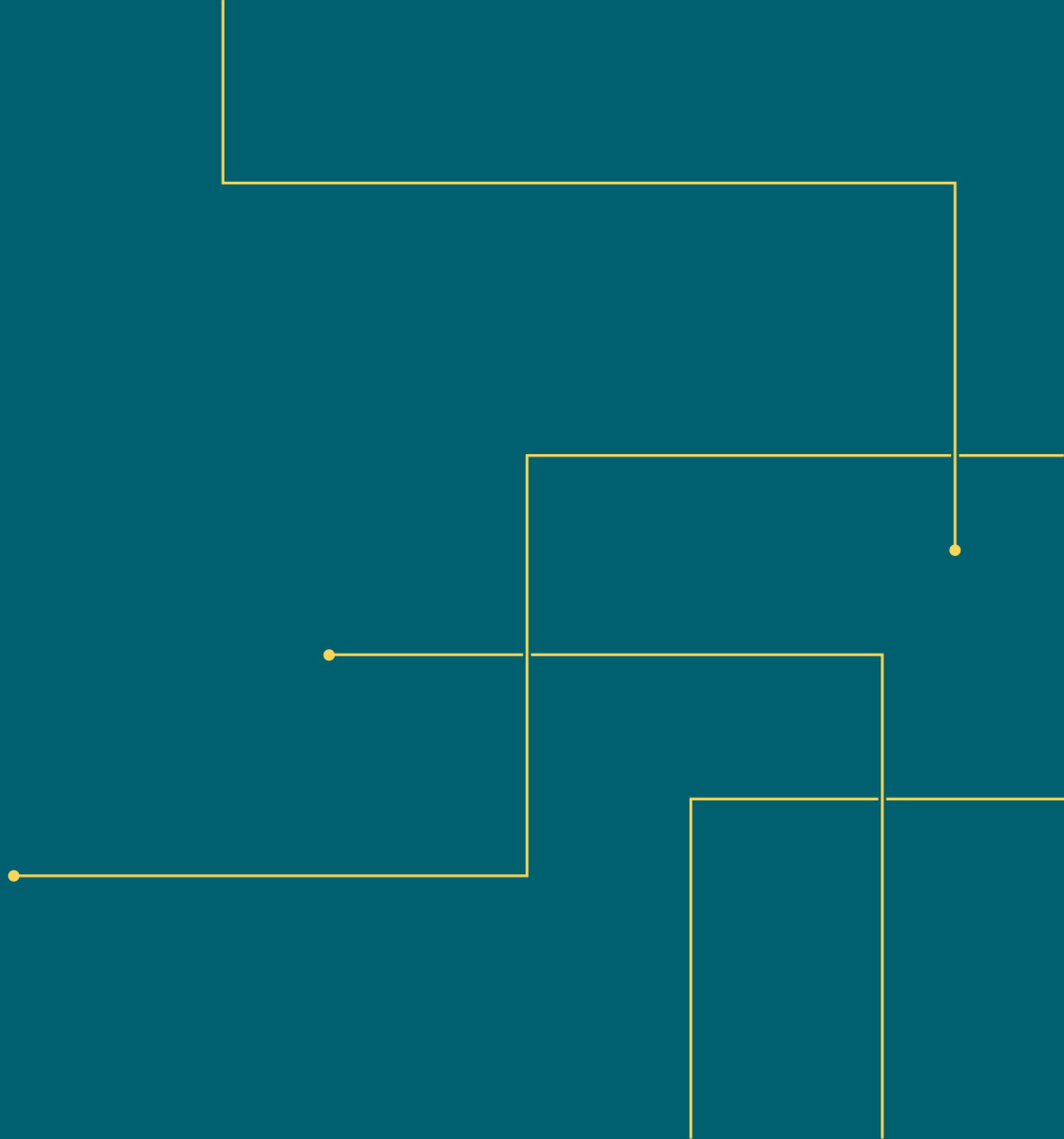
State: Floor/Suite:



STEPS NEEDED (CONT)

- When returning from international travel, do not reconnect any device that was taken abroad to the agency network. The loaner device and or MiFi will be contained and sanitized as a result of the KSE workflow before it should be reissued or placed in use.

QUESTIONS?



CYBERSECURITY AWARENESS TRAINING FOR THE COMMONWEALTH

Tina Gaines

CSRM



- What VITA has completed:

- Knowbe4 Training:

Training on KB4 started 3/29 with six agencies in attendance. There will be weekly training sessions for admins to help them become familiar with setting up their training campaigns. The goal is to schedule 10 agencies at time until all admins are trained. Admins will be notified in advance of their scheduled training date. The dates are as follows:

Thursday, April 6

Thursday, April 13

Monday, April 17

Thursday, April 27

Note: Training sessions will be from 1:15p – 1:50p. Individual agency sessions will also be made available once the initial training sessions are completed.



- Additional Training Dates:

- Knowbe4 Training:

- If you did not attend any of the training last month, VITA has secured additional training dates. We strongly encourage console admins not familiar with KB4 to attend one of the training sessions.

- The dates are as follows:

- Wednesday, May 10

- Wednesday, May 17

- Wednesday, May 24

- Monday, May 27

Note: Training sessions will be from 1:15 – 1:50 p.m. Individual agency sessions will also be made available once the initial training sessions are completed.



- The agency should:
 - Generate reports to close out their current training solution for audit purposes.
 - Start uploading your users to the KB4 platform
 - Create a preliminary test campaign
 - Create a test group to assign training to

How to Get Started with KnowBe4 Console:

<https://support.knowbe4.com/hc/en-us/articles/115011714508>

<https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/pdf/KnowBe4-527-Crosswalk.pdf>

- Phase One – Those agencies who are currently subscribed to Knowbe4. This phase will take place the week of **January 30, 2023**. Phase one included over 20 state and independent agencies, two higher ed agencies, the Governor’s Office, and two agencies who did not use Knowbe4 as their training solution
- Phase Two (**Month of March**)– Majority of the agencies not included in phase one. This phase is scheduled to be completed by **July 2023**.
- Phase Three – This phase will include agencies that might be a little more complex, challenging, or their subscription renewals expire later in the year or next year. This phase is scheduled for completion by **December 2023**.



KNOWBE4 PRODUCT UPDATES

New Feature! Executive Reports

We're excited to announce the Executive Reports feature that lets your team create, tailor and deliver advanced executive-level reports to help your organization make efficient data-driven decisions regarding your security program. Use one of three executive report templates, or create your own, to visually represent areas of success and improvement, measure risk, and even include your own recommendations.

With Executive Reports You Can:

1. Efficiently access and share key data metrics about your security awareness training program
2. Present security insights to show the effectiveness of your security program and demonstrate ROI
3. Save and schedule updated reports to automatically send as a PDF on a recurring basis
4. Tailor reports to a specific audience providing relevant data for actionable results

Now it's easy for your executives to be in the know when it comes to the overall success of your security awareness and culture program across your organization! The Executive Reports feature is included in all KMSAT subscription levels.



KnowBe4 – Introduction to Cybersecurity in the Metaverse

The concept of the metaverse has been around for decades but has exploded in popularity in the last few years. The word "metaverse" is thrown around a lot, but what does it mean? In this module, users will explore what the metaverse is and what you need to know to protect yourself before you dive into this virtual frontier.

Sign up to preview this content now:

<https://info.knowbe4.com/security-awareness-training-preview-monthly-update>

Four new pieces of training content added this month. The Introduction to Cybersecurity in the Metaverse module is available across the Gold, Platinum and Diamond subscription levels.



Popcorn Training – Spot the Phish Game: Reloaded

Choose your hero and help them spot the phish! Steal lives from the cybercriminal in this exciting game that teaches your users how to spot warning signs in digital correspondence. From QR codes to text-based phishing and everything in between.

Sign up to preview this content now:

<https://info.knowbe4.com/security-awareness-training-preview-monthly-update>

Three new pieces of training content added this month. Training content from Popcorn Training, including Spot the Phish Game: Reloaded, is available at the Diamond subscription level.



TOTAL SECURITY AWARENESS CONTENT

Ready to see how you can build a mature security awareness training program using great, fresh content from the KnowBe4 library?

As of April 26, 2023,
KnowBe4 has over

22,000

phishing and landing
page templates

337

Interactive Training Modules

562

Video Modules

245

Posters and Artwork

277

Newsletters and Security Docs

1446

Pieces of Education
and Training Content

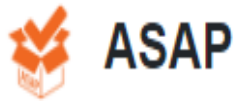
25

Games



KNOWBE4

ASAP (AUTOMATED SECURITY AWARENESS PROGRAM)

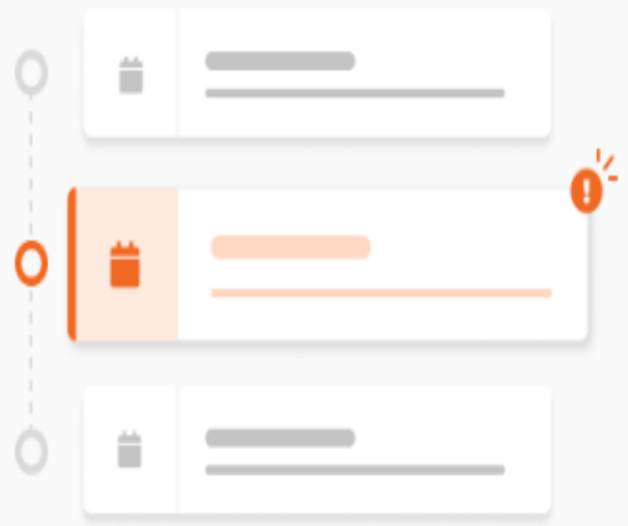


Start your Automated Security Awareness Program (ASAP)

Create a customized security awareness program for your organization in just minutes. Your ASAP includes step-by-step instructions and recommended training content tailored to your specific needs.

[Get Started](#)

[▶ Watch Video](#)





Question 1 of 7

What are your training goals for this program?

This allows us to recommend content and step-by-step instructions that will help you meet the specific training goals of your organization. Select all that apply.

Security Awareness Training
Training to educate users about security awareness concepts and best practices.

Compliance Training
Training to meet compliance or regulatory requirements.

Physical Security Training
Training that covers clean desk policies, tailgating, locking devices, and more.

HR-related Training
Training to educate users about workplace violence, sexual harassment, and more.

Next



Question 2 of 7

What security awareness activities have you already started?

Let us know if you have phished or trained your users in the past, or if you have established an email incident response plan. If you haven't yet, don't worry! We'll walk you through how to start these activities, step by step.

Simulated Phishing Tests

How often do you currently send simulated phishing tests to your employees?

Quarterly



Security Awareness Training

How often do you require your employees to take security awareness training?

Annually



Incident Reporting

How does your organization currently handle email incident response?

- We have a process for users to report suspected phishing emails.
- We review reported emails and respond to users.

Next

Back

Which training topics would positively impact your organization?

Consider the positive impact you want your security awareness program to have in your organization. Select at least two behavior changes that you would like to see in your users as a result of your program.

Human Firewall

▼ Details

Working Remotely

▼ Details

Data Privacy

▼ Details

Discrimination

▼ Details

WiFi

▼ Details

Incident Reporting

▼ Details

Physical Security

▼ Details

Data Protection

▼ Details

Diversity, Equity & Inclusion

▼ Details

Internet Use

▼ Details

Ethics

▼ Details

Employment Law

▼ Details

Mobile Devices

▼ Details

Workplace Safety

▼ Details

NIST

▼ Details

Email Security

▲ Details

Train users on how to identify phishing emails and other email-related cybersecurity attacks.

Social Media

▲ Details

Train users to avoid risks associated with using social media platforms.

Personal Security

▼ Details

Red Flags

▼ Details

Passwords & Authentication

▼ Details

Harassment

▼ Details

Next

Back

What types of data, legislation, or regulatory standards should be considered?

We offer training content to cover a variety of regulatory, industry, or compliance standards. We will include this in your customized plan. Select all that apply.

POPIA
Protection of Personal Information Act

FMLA
Family Medical Leave Act

GDPR
General Data Protection Regulation

NERC
North American Electric Reliability Corporation

FERC
Federal Energy Regulation Commission

HIPAA
Health Insurance Portability and Accountability Act

FERPA
Family Educational Rights and Privacy Act

LGPD
Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais)

PII
Personally Identifiable Information

PCI
Payment Card Industry

PIPEDA
Personal Information Protection and Electronic Documents Act

PHI
Protected Health Information

FCPA
Foreign Corrupt Practices Act

None of these

Next

Back

Which job roles would you like to provide specific training for?

We offer a variety of role-based training content to support users in specific roles. Select the roles that you want to provide training for and we will include this as part of your customized program.

Customer Service Team
Training for employees who work directly with customers and may have access to sensitive data.

Developers
Training for developers and programmers. Topics could include securing web applications, threat modeling, and more.

Finance Staff
Training for employees on your Finance or Accounting teams.

Frequent Travelers
Training for employees who travel frequently.

IT Staff
Training for employees on your Information Technology team.

Payment Card Processors
Training for employees who need to process debit or credit cards.

Executives & Leaders
Training for executives and leaders in your organization.

None of these

Next

Back

Which training styles best fit your organization's culture?

Your organization's culture is unique and your security awareness program should reflect that. Choose the training styles that match your organization's culture and we'll include them in your customized program.

Animated

Vivid and engaging content that helps capture the attention of your users.

Interactive

Engaging content that includes quiz questions, games, and other interactive training features.

Live-Action

Content that uses live actors to engage your users in their training.

Conventional

Straightforward training that only gives your users the facts.

Humorous

Content designed to be memorable and fun, so users remember important information.

Next

Back

Which of the following items apply to your organization?

Select all of the items that you'll have to consider when implementing your new program and we'll build a plan that supports your specific setup.

We have an internal approval process for simulated phishing, training, or changes to technical controls. [Details](#)

We use multiple spam filtering solutions. [Details](#)

We haven't whitelisted KnowBe4 or haven't tested our whitelisting. [Details](#)

We use a firewall to block outbound traffic. [Details](#)

We haven't verified that we can track clicks from KnowBe4's simulated phishing emails. [Details](#)

We use a link analysis or URL rewriting service. [Details](#)

We need to add our users to our KnowBe4 console. [Details](#)

We want to brand or customize KnowBe4's training content. [Details](#)

We have our own training content that we want to use in our KnowBe4 console. [Details](#)

None of these

[Generate Program](#)

[Back](#)



Your Security Awareness Program Tasks

Based on your questionnaire answers, we generated a customized program for your organization. Follow the steps below to implement your program.

Task List

☰ Task List

📅 Calendar

Next Task

May
5**Engage your stakeholders**

about 2 hours ▾

Upcoming

Completed

May
8**Customize your KnowBe4 console**

30 minutes ▾

May
23**Whitelist KnowBe4's mail servers**

Variable ▾

May
31**Add users and create groups**

about 4 hours ▾

Jun
8**Create and complete a baseline phishing campaign**

30 minutes ▾

Jun
9**Review the results of your phishing test**

30 minutes ▾

Virginia Department of Conservation and Recreation

Organization Information

The information below was used to generate your organization's customized program.



Industry

No industry on file.



Organization Size

583



User Languages

Your account's default language and most used languages are listed below.

Top Phishing Languages

- English (United States) **Default**

Top Training Languages

- English (United States) **Default**

Questionnaire Responses

Each question below includes the responses provided when your ASAP questionnaire was originally completed.

Question 1

Question 2

Question 3

Question 4

Question 5

Question 6

Question 7

What are your training goals for this program?

- Security Awareness Training
- Compliance Training
- Physical Security Training

ASAP Settings



Start Date

If you change the start date, all the tasks in your program will be automatically updated based on the start date.



04/27/2023

Save

Reset Program

If you would like to start a new program, click the Reset Program button below.


Reset Program

May 2023

Today



Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
30	1	2	3	4	5	6
Engage your stakeholders						
7	8	9	10	11	12	13
	Customize your KnowBe4 cc		Whitelist KnowBe4's mail servers			
14	15	16	17	18	19	20
Whitelist KnowBe4's mail servers						
21	22	23	24	25	26	27
Whitelist KnowBe4's mail servers			Add users and create groups			
28	29	30	31	1	2	3
Add users and create groups				Create and complete a baseline phishing campaign		
4	5	6	7	8	9	10
Create and complete a baseline phishing campaign					Review the results of your phishing test	

May
5Engage your stakeholders 

Description

To have the most success with your security awareness program, involve your stakeholders at the beginning. When your stakeholders understand your program, they can act as advocates and help to answer employee questions or make sure employees complete training on time.

To engage your stakeholders:

Identify your stakeholders:

- Your stakeholders are usually your C-level executives and department managers.

Gather your resources:

- Download your **ASAP Executive Summary Report**. Click the **Download PDF** button to download this customized report, which provides details about your new partnership with KnowBe4.
- Download our **Security Awareness Training Policy** template, provided in the Resources section. This template can help you create an internal policy that will support your program's goals.

Meet with stakeholders:

- Schedule a meeting to introduce your program to your stakeholders.
- Provide a copy of your Executive Summary Report to each stakeholder.
- Explain how you plan to implement your program in your organization.

Send a follow-up email:

- Copy and customize our **Engage Your Stakeholders** template, provided in the Resources section.
- Email your customized template to your stakeholders.



Resources

- [How Can I Engage My Stakeholders?](#)
- [Customizable Security Awareness Policy Template](#)
- [Forrester: The Total Economic Impact of KnowBe4](#)

Start Date

April 28th, 2023 

End Date

May 5th, 2023 

Estimated Duration

about 2 hours

[Mark Complete](#)



MAY 3, 2023

COMBINING SEC501-SEC525

UPDATE

ALSO KNOWN AS SEC530

BY: CHANDOS CARROW

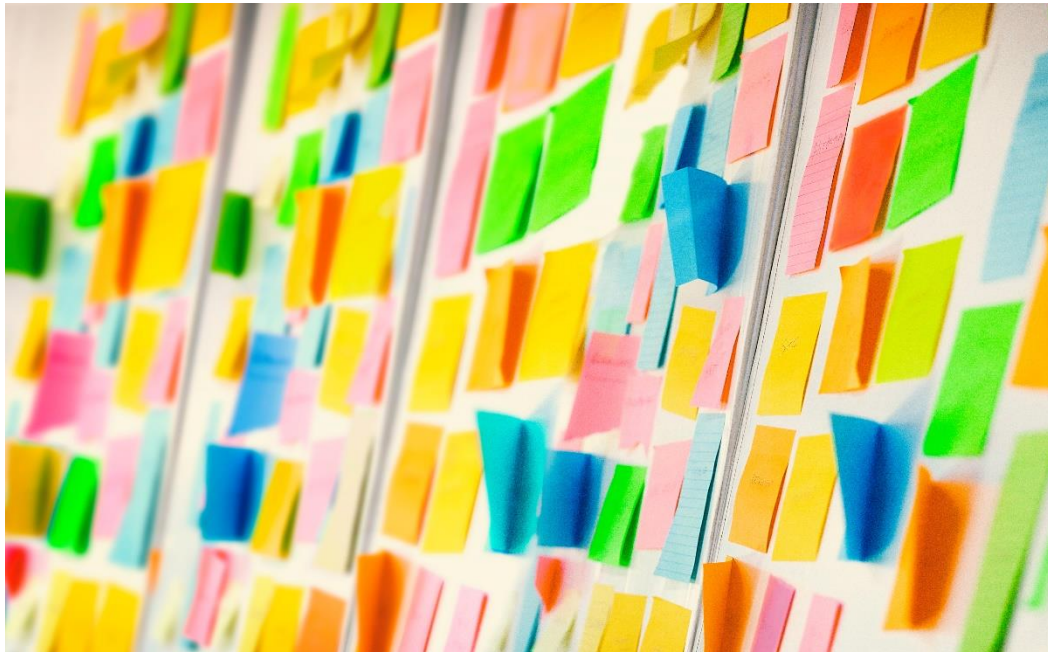
VITA/CSRM Acting Security Architect Team Lead

MAY 2023 ISOAG



- The review committee is on SI-4.
- The ISO Council has been provided control families AC through PL to review.
- Reviewing feedback from various agencies.





- Still must review:
 - Remaining controls in SI
 - The new Supply Chain Risk Management control family
 - Sections one – seven
 - Any follow-ups previous identified
- Present at AITR meeting the major changes coming with SEC530
- Submit to ORCA



THANK YOU!



Chandos Carrow

chandos.carrow@vita.virginia.gov



UPCOMING EVENTS

[IS Orientation](#)

[Remote - WebEx](#)

Date: June 28, 2023

[Start time: 1:00 p.m. End time: 3:00 p.m.](#)

[Instructors: Erica Bland, Renea Dickerson and Tina Gaines](#)

<https://covaconf.webex.com/weblink/register/rbc9d847b4c8579e4428f406f6275ae>

[b9](#)

The next scheduled meeting for the IS Council:

May 17, 2023

12 - 1 p.m. (virtual)

If you would like an invite to the meeting, contact:

tina.gaines@vita.virginia.gov



COMMONWEALTH OF VIRGINIA
**INFORMATION SECURITY (IS)
CONFERENCE 2023**



**Revolutionizing IS through Advanced Thinking:
Unleashing the Power of Human Ingenuity and AI**

Save the date for the most innovative Commonwealth of Virginia Information Security conference, yet!

Date: August 17, 2022

Time: 8 a.m. – 3 p.m.

Cost \$125

Location: Hilton Richmond Hotel and Spa/Short Pump at 12042 West Broad Street, Richmond, VA 23233.

Join us for a day of thought - provoking discussions and networking opportunities with industry experts.

Keynotes:

Paul Chin Jr., Serverless Developer (Chat GPT)
Elham Tabassi, NIST (NIST AI Framework)



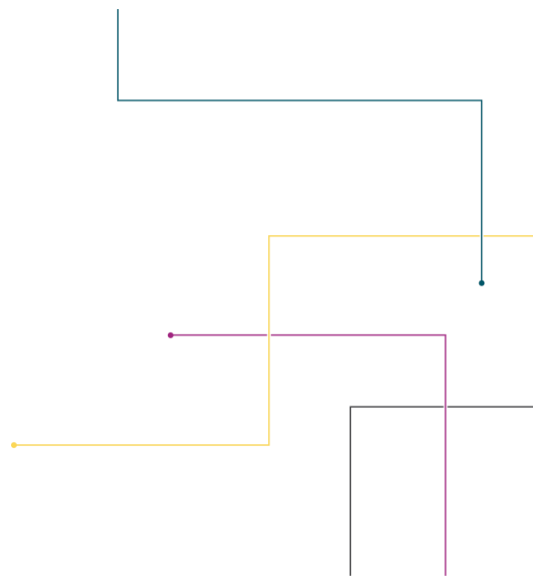
JUNE ISOAG MEETING

June 7, 2023

TIME 1 P.M. - 3 P.M.

SPEAKERS: TBA

**MEETING
ADJOURNED**



**VIRGINIA
IT AGENCY**