Splunk Inc., Information Technology Solutions (ITS) PMO

Project Communications and Process Improvement

I was embedded in Splunk's ITS PMO and drove project communications for the **Endpoint Security Protection (ESP) program**, distilling complex, technical information into crisp, clear language with as little jargon as possible in support of the program director and five project managers across nine workstreams. Our internal clients were technology and engineering teams, the ITS leadership team, and the SGS (security) leadership team. (Endpoints—desktops, laptops, smartphones, tablets, servers, and workstations—are key points of vulnerability and provide attack paths into corporate networks by cybercriminals.)

I came aboard the ESP program two months in and served seven months, to the end of the program. I created and led a hands-on communications framework to strengthen Splunk's ESP transformation journey:

1. It was clear when I started on April 1 that there was confusion among ESP team members regarding how they would use a project communications resource, as opposed to existing communications resources, including the nascent change management team or the brand management team that sat in corporate communications. On my third day, April 3, I created the first slide in the pages that follow to make the necessary distinctions, to good effect.

2. My second task was to nurture productive, collaborative relationships with technology and engineering teams, which called attention to grave inefficiencies in the content creation and distribution process. To address the issue, I introduced a light-touch, repeatable process that increased predictability, consistency, and accountability, creating fewer pauses and roadblocks that were killing content distribution timelines. That light-touch process, which is illustrated in the two communications samples enclosed, was built on the commitment of my technology and engineering colleagues to meet by Zoom for 45 minutes at project kickoff to gain a solid footing and common understanding among ITS and SGS leaders and subject matter experts regarding the communications support, which was especially important because most communications support required a series of communications.

   The most interesting example thereof was the initiative for bringing Linux endpoints into compliance, a critical element of the Endpoint Security Protection (ESP) program, as mandated by SpAARC, Splunk's audit committee. The Linux initiative was kicked off on June 10 and completed on August 18, the day HIP (Host Identity Protocol) checks were enforced, which meant that users who delayed in acting were locked out of the network. To get the cooperation of our Linux community, which was a tough task, we employed a simultaneously white-glove and threatening approach because Linux users are the Splunk's application developers and therefore Splunk's moneymakers, a great many of whom have been around since the company's inception and are used to working in a wild west environment.

ESP's Symphony of Communication

Communicating company messages, especially messages of change, threaten the status quo.

Organizational Change Management

Organizations today are in a constant state of flux as they respond to the fast-moving external business environment, local and global economies, and technological advancement. Splunk is no different. This means that workplace processes, systems, and strategies must continuously change and evolve for Splunk to remain competitive. Change management is no longer a term that denotes only operational improvements, cost efficiencies, and process reengineering. Change management has become a much larger, more interwoven part of the overall business fabric and is now an embedded leadership requirement that plays into everything the organization undertakes. Managed change and a well-designed change management plan can support a smooth transition and ensure that employees are guided through the change journey.

Here are the five steps of an effective organizational change management plan:

1. Clearly define the expected change and how the change aligns to business goals.
2. Determine the impacts and those affected.
3. Develop a communication strategy:
   Key questions:
   - How will the change be communicated?
   - How will feedback be managed?
4. Provide effective training:
   Key questions:
   - What behaviors and skills are required to achieve business results?
   - What training delivery methods will be most effective?
5. Measure the change process.

Change is personal and emotional. Organizational change management brings behavioral psychology to bear, delivering an engagement model that helps cut through the noise. Thoughtful managed change will:

- Deliver project results
- Increase transparency
- Increase the probability of success
- Manage employee resistance
- Minimize the impact of productivity losses
- Minimize the loss of valued employees
- Build change competency into the organization
- Enhance brand reputation

Project Management Communications

Project management is about implementation, while, as described above, organizational change management is about adoption. Project communications is a collection of processes that help ensure that the right messages are sent, received, and understood by the right project stakeholders. Project communications is one of the 10 knowledge areas defined in PMBOK (the Project Management Book of Knowledge). The processes defined in the current, 7th edition, include three project communications processes: (1) Plan Communications Management, which is focused on creating a communication plan, (2) Manage Communications, which is focused on plan execution, and (3) Control Communications, which is focused on measuring and refining communications. The benefits gained from a disciplined approach to project communications include:

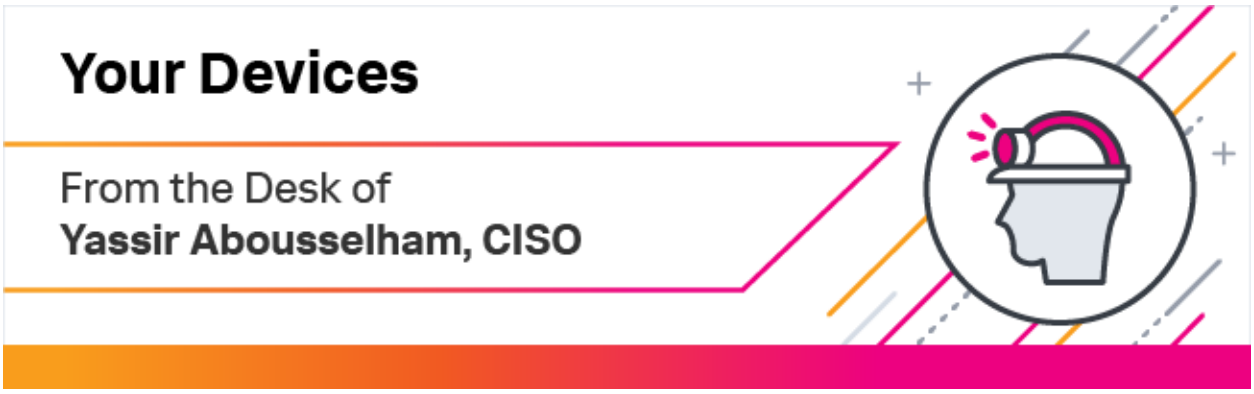
- Strengthened internal information exchanges (i.e., decision-making processes)
- Strengthened information management (i.e., communication with project stakeholders and leadership teams)
- Strengthened project marketing communications (i.e., project presentation to employees, leaders, and sponsors)

Internal Brand Management

Strong brands communicate strong ideas. Visual communications unify messaging and are beneficial because they subtly hint at a promising and unified path forward. In this way, internal branding creates a relationship between the brand and our employees, essentially unlocking many unspoken or rarely spoken mysteries of the organization that demonstrate how integral each employee is to delivering on the corporate mission. A strong, unified internal brand will:

- Improve program and mission focus
- Strengthen organizational and operational leadership
- Deepen employee connection to the organization
- Improve hiring and retention
- Break down organizational silos
- Create ardent brand advocates

splunk> turn data into doing



Guidance for High-Risk Travel

Travel involves many inherent risks. For the safety and security of our employees, we ask you to plan your trips accordingly and to exercise commonsense caution when on the road.

Travel to high-risk regions is more complex than general travel due to the possible threats posed to Splunk's network infrastructure and therefore requires an even more heightened level of preparation and vigilance.

Splunk defines "high-risk countries" (HRCs) based on guidelines from the United States Department of Homeland Security and the United States Department of State.

Whenever You Travel, Wherever You Travel, Travel with Safety in Mind

While this guide calls out specifics related to high-risk travel, all travel (domestic and international) requires caution. Staying safe requires that you exercise common sense and situational awareness.

We have broken this guide into three sections to call out recommendations and reminders for safe and productive travel:

Section 1: What You Need to Know about Travel to High-Risk Regions

EXERCISE CAUTION WHEN TRAVELING TO HIGH-RISK REGIONS

- Employees who travel to countries listed in the **High-Risk Travel Policy** must adhere to the directives found within the policy. Therefore, travel to high-risk countries requires special consideration and preparation. The aforementioned policy also includes a list of those regions identified as high risk.

- Splunk will issue loaner laptops to employees to perform duties while in high-risk areas. Those

devices will have enhanced or additional security measures, as outlined in the policy.

- To provide our travelers with trouble-free support, we require travelers to use our centralized online booking system, **Egencia** or their local **Egencia partner**. Using Egencia ensures access to all of Splunk's travel-related services.

- If you want to access Splunk systems from your personal phone while traveling to a high-risk region, you must have IT install Advanced Mobile Device Management software on your mobile device. You can submit the request through ServiceNow.

BOOKING YOUR TRIP TO A HIGH-RISK REGION

Because travel to high-risk regions is evaluated more aggressively than regular international travel, we recommend that you book your trip and request your loaner laptop **at least 10 business days** in advance of your travel date to ensure your trip goes smoothly. Here are the specifics you need to know:

1. Travel requests to high-risk regions are automatically flagged by Egencia.

   Note that travel requests to non-high-risk countries pass through the system uninterrupted.

2. The requestor will receive a popup during the booking process with information about the policy and notification that a loaner laptop has been requested for her or him. A follow-up email will be sent to the traveler and his or her manager with the ServiceNow ticket number and support options.

WHAT ADDITIONAL HELP IS AVAILABLE TO ME?

We encourage you to download **WorldCue Mobile**, which is a **multilingual** smartphone app (iOS and Android). Here is what you need to know about WorldCue Mobile:

- **WorldCue Mobile automatically syncs with Egencia**, providing you with multilingual security alerts and immediate access to travel intelligence and assistance.

- With WorldCue Mobile and Egencia, you get 365/24/7 assistance, including:

  - Medical assistance, if needed
  - Evacuation alerts, if necessary
  - Pre-trip briefings, to include health information, political stability, and travel information
  - Alerts and updates on any changes affecting ALL legs of your trip

- Here is how to download the app:

  - Go to the **iOS App Store** to download the app on your Apple smartphone
  - Go to the **Google Play Store** to download the app to your Android smartphone

Section 2: Exercising Heightened Awareness Wherever You Travel

PREPARING FOR YOUR TRIP

- Confirm your ServiceNow (SNOW) request for a loaner laptop if you are traveling to a designated high-risk region. (As noted above, Egencia will automatically generate a SNOW ticket and follow up with an email confirmation. Refer to that email for additional instructions and contact the Service Desk

if you do not receive the confirmation email.)

- Re-review the Splunk Acceptable Use Policy to re-familiarize yourself with Splunk's cybersecurity expectations.

THINGS TO REMEMBER WHILE TRAVELING

- Immediately file an incident report with the **Global Security Coordination Center (Slack #GSCC) or call +1-571-421-6783** if your laptop has been lost, stolen, confiscated, or compromised. Other reportable security incidents include malware, keylogging, ransomware, compromised user account, or denial of service.

- Here are additional recommendations for safer, more secure travel:

    - ★ Be mindful of public Wi-Fi hotspots and connect only when necessary. **Mac users** can set Wi-Fi to "do not automatically connect" by clicking the Wi-Fi icon in the upper righthand corner and clicking the slider. **Windows users** can turn off automatic connections by selecting the Start Menu, then following this navigation: Settings / Network & Internet Settings / Wi-Fi.

    - ★ Do not update software on your computer while connected to a public or hotel wireless network, even if prompted to update.

    - ★ Be mindful of your device and screen at all times, especially in public areas and when logging in or inputting data into your devices. Use the provided privacy screen when on your laptop, and never leave your laptop or mobile device unattended.

    - ★ For passwords, do not use the "remember me" feature; instead, manually retype your password when prompted.

    - ★ Do not post about your travel plans to social media before or during your travel, and do not post from a country designated as a high cybersecurity risk.

    - ★ Avoid transporting devices in checked baggage.

    - ★ Do not open unsolicited emails or attachments, and do not click on links before verifying the source is legitimate. If you have questions about verifying emails, refer to the Phishing Attacks - Security Advisory. When in doubt, please forward the email in its entirety to phishing-pond@splunk.com.

    - ★ Shut down the laptop when it is not in use.

WHEN YOU RETURN

- Immediately change any passwords you may have used during your travels to prevent future attacks on your account.

- Do not use the laptop you traveled with to reconnect to the Splunk network. Ensure that the laptop is wiped and reimaged by the Global Service Desk with trusted software versions.

Section 3: Frequently Asked Questions (FAQs)

What countries are covered under our High-Risk Travel Policy?

Splunk defines “high-risk countries” (HRCs) based on guidelines from the U.S. Department of Homeland Security and the U.S. Department of State, and we will update our list accordingly. To see the most current list of high-risk countries and regions, as identified by Splunk, please go to the **High-Risk Travel Policy**, which will always be kept up to date.

What happens if my manager has an issue with possibly limited productivity while I am away?

Although loaner laptops will be restricted, they will still provide access to standard corporate applications and systems. However, some features will be disabled, such as remote login (SSH), remote management, and the ability to install additional applications. Contact the Service Desk at #help-servicedesk for a complete list of restrictions. Please discuss this issue with your manager well in advance of your travel plans to determine if your productivity will be impacted and how you can mitigate any impact to your work.

What if I forget to add advanced mobile device management (MDM) to my mobile device before I leave?

Please contact the Service Desk at #help-servicedesk ASAP to be added to the advanced MDM group.

What happens if I accidentally bring my work laptop instead of or in addition to the loaner?

Please contact the Service Desk at #help-servicedesk immediately, and they will advise you on next steps, depending on your specific situation.

What do I do if my device is breached, confiscated, or if there is unauthorized access to the network?

In the event of a security incident, immediately file a report with the **Global Security Coordination Center (Slack #GSCC) or call 1-571-421-6783.** Reportable security incidents include lost, confiscated, or stolen laptops, malware, keylogging, ransomware, compromised user accounts, or denial of service.

Will loaner phones or tablets be available for travelers to high-risk regions?

At this time, Splunk will not be issuing loaner phones or tablets.

Document Title	Guidance for High-Risk Travel	
Document Owner	Yassir Abousselham, CISO	
Policy Stakeholders	Splunk IT Data Protection – Legal Splunk Travel Splunk Physical Security	
Launch Date	03/22/2021	
Document Objective	Develop easily digestible, easy-to-understand guidelines for overseas travel overall and high-risk travel in particular, the latter of which will include security guidelines, including the loaner laptop requirement	
Audience	Splunkers who book their travel through Egencia	
Delivery Methods	1. For Splunkers seeking guidance before booking travel: Document will be hosted on SGS's Google Drive folder and posted to the SGS landing page on Pwny Portal. 2. For Splunkers requesting travel to high-risk regions on Egencia: An automated popup from Egencia will direct the Spunker through the process for travel to high-risk regions, including the loaner laptop requirement	
Document Approval Process	Creation	Peter Speliopoulos Consultant, IT PMO, Endpoint Security Protection (ESP)
	Review	Joy Anzinger Director, Corporate Travel & Expense
	Review	Tanya Pfeffer Senior Manager, Client Platform Engineering, Splunk IT
	Review	Tony Iacobelli Senior Security Incident Handler, SGS
	Review	Meera Shankar Senior Risk Analyst, SGS
	Approval	Yassir Abousselham, CISO

Message for Slack (Must Be Splunkified for the Pwny Portal

Hello, Splunk people manager! Did you know that Splunk IT has deployed more than 1,000 laptops to our new starters over the last two quarters? Although growth is exciting, managing the employee lifecycle can sometimes pose challenges. As part of a recent effort to ensure that we are quickly shipping systems to users, it is equally important that we receive those devices when employees separate. As part of your offboarding conversations, **we ask that you remind exiting employees of their responsibility for returning their Splunk-owned assets**. Please take a minute to review this Manager's FAQ, which shares recent advancements made to streamline the asset reclaims process.

Manager's FAQ

Manager's FAQ: Recovering Laptops from Employees Who Leave Splunk

Employee turnover is a fact of life, and asset retrieval is the responsibility of every Splunk manager. It is therefore important for you to be ready for this eventuality.

Here is what you need to know to ensure that separating employees (Splunk alumni) return their Splunk-issued laptops:

What does the employee separation process look like?

Employee separation is a five-step process:

1. The process begins with the employee's decision to separate or the manager's decision to terminate.
2. Next, the employee's profile is updated, as follows:
    a. For fulltime, permanent employees (FTEs), the Splunk People Operations Team (SPOT/HR) will process the termination in Workday.
    b. For alternative workforce resources (e.g., contractors), managers are responsible for processing the offboarding in the Wand/AWF portal.
3. An offboarding ticket is created in ServiceNow, alerting the Service Desk to:
    a. Revoke systems access to account(s)
    b. Track the return of Splunk equipment
4. The separating employee is sent instructions or packaging for prepaid shipping with FedEx (or a local shipping vendor, depending on the Splunk alumni's region).
5. Finally, the Service Desk will track the return of the package, from dropoff at FedEx to delivery at Splunk.

What specifically is expected of managers?

The requirements are limited:

1. **Voluntary separations (i.e., the employee gives notice or resigns):** Managers are expected to initiate a separation request in Workday (or work with SPOT/HRBP to do so) when an employee submits his or her resignation.
2. **Involuntary separations (i.e., termination for cause, performance, etc.):** SPOT or your HR business partner will initiate the termination process in Workday for all involuntary terminations.
3. Next, we ask that managers communicate directly with the departing employee, clearly laying out the expectation that Splunk-owned equipment must be **returned within seven days** of the employee's last day of work.
4. SPOT/HR, the Service Desk, and Global Security coordinate the details of equipment return and will send an email to separating employees with specific instructions or packaging for prepaid shipping with FedEx.

How long does a separating employee have to return his or her laptop?

Splunk equipment is expected to be dropped off at a FedEx location for return delivery within **seven (7) days** of the employee's last day worked.

We request that our managers lay the groundwork for separating employees with strong, but sympathetic, guidance by asking departing employees to start preparing for the return of their Splunk laptops during the week leading up to their last day of work. This includes reminding departing employees to:

1. Download their personal data to an external drive
2. Transfer ownership of their work files and drives to their direct manager and teammates

What should managers do if a departing employee reports that the shipping material has not been received?

In situations where the separating employee has not received her or his Splunk hardware instructions or packaging, we ask that managers reach out to the Splunk Service Desk for assistance in completing the asset reclamation. When a manager reaches out to the Service Desk, the situation will be investigated, and the Service Desk will follow up with the separated employee. No further action is required of the manager.

What if I need additional help in recovering Splunk-owned assets or if I have questions about the asset reclamation process?

If you run into roadblocks, have questions, or want to know the status of an asset reclamation, please select one of the following resources:

1. Inquire in the Slack channel #help-service desk
2. Call 1-877-371-8267 for 24/7 support
3. Email help@splunk.com and a ServiceNow ticket will automatically be created for you

Thank you for supporting the asset reclamation process!

Document Title	Recovering Laptops from Employees Who Leave Splunk	
Document Owner	Ashley Sprague, Senior Director, IT Operations	
Policy Stakeholders	IT Operations Legal	
Launch Date	04/08/2021	
Document Objectives	1. Remind managers of their responsibility to notify separating employees of the need to return their laptops 2. Notify managers that the separation process is now fully articulated and addresses the lack of information that has been available to managers 3. Provide managers with overview of the separation process, including communications that will be sent by SPOT	
Audience	Splunk people managers	
Delivery Methods	1. Managing@Splunk on the Pwny Portal 2. #people-managers on Slack	
Document Approval Process	Creation	Peter Speliopoulos Consultant, IT PMO, ESP
	Review	Earlvin Rivera, IT Business Systems Analyst, Corporate Finance
	Review	Jeff Johnson, Project Manager, IT PMO, ESP
	Review	Karan Bajaj, Director, IT PMO, ESP
	Review	Agim Kraja, Senior Manager, Global IT Services and Support
	Approval	Ashley Sprague, Senior Director, IT Operations