IT NATION™ SECURE

hosted by CONNECTWISE®

The Shortcut to Big Profits in CMMC Compliance Without Hundreds of Hours of Study and Documentation Writing

Presented by: Leia Kupris Shilobod, CPP, CISM

IT NATION™ SECURE

Today We're Going To Cover:

- The 5-step process to create a solid CMMC Compliance offering that will blow your competition out of the water and get your clients to pass their CMMC Assessment.
- The easy secret to create the required CMMC Policies, Plans, and Procedures
- The fool-proof method to get and keep your clients compliant
- Avoid painful mistakes, client finger pointing, and lawsuits for wrong compliance decisions
- Tips to access the powerful CMMC community and brilliant mind-share to never feel lost in your CMMC Compliance Program

Who Is Leia Kupris Shilobod?

InTech SOLUTIONS

CMMC IT Documentation Toolkit

"I am a cyber security, documentation, and compliance professional who specializes in helping companies to **standardize** and **secure** their **IT infrastructure and processes** for companies with less than 2,000 endpoints."

- Founded InTech as a Security focused MSP in 2006
- Speak country-wide on IT Security, IT Documentation, IT Operations, CMMC | NIST 800-171, and IT for Manufacturers
- Process Driven
- CMMC RPO, Certified CMMC Professional (CCP), Certified Information Security Manager (CISM)
- Author of the **"CMMC IT Documentation Toolkit"**
- Co-Star and Co-Producer of move **"Cybercrime: The Dark Web Uncovered"**
- Author of 2 Books:
  - "Cyber Warfare: Protecting Your Business From Total Annihilation"
  - "The 3 Indisputable Rules Every Manufacturer Must Know Before Purchasing Any IT Product or Service"

INFRAGARD PARTNERSHIP FOR PROTECTION

CISM

CYBER AB
REGISTERED PRACTITIONER ORGANIZATION
RPO

#ITN

IT NATION

DISCLAIMER:

What I'm going to share with you today is what's worked for my company doing this work for the last 5 years, and after hundreds of hours of study and learning, and literally thousands of hours of trial and error.

You DO NOT have to use my method to create a CMMC Compliance Program. BUT if you want the shortcut, I can teach it to you…

Don't Miss The Opportunity

"What's the biggest trend MSP's should pay attention to right now?"

"COMPLIANCE IS COMING"

Fred Voccola, CEO
Kaseya

#ITNation

What CMMC Is

- The Cybersecurity Maturity Model Certification
- Required cybersecurity for any contractor dealing with Federal Contract Information (FCI) AND/OR Controlled Unclassified Information (CUI)
- A maturity model of Basic to Advanced cybersecurity practices
- A cybersecurity compliance PROGRAM
- A journey, not a destination
  (any client ever ask you “Am I secure yet?”)

What CMMC Is NOT

- Something to “wham, bam, thank you ma’am” to make a quick buck
- An infrastructure upgrade project
- GCC High (oh man do not get me started)
- Anything “in a box”
- A toolset
- Something a company can outsource or “set and forget”

The CMMC Opportunity

- Over **200,000 companies** in the Defense Industrial Base (DIB) need to be compliant with CMMC
- The vast majority **need an MSP**, most also need **help with CMMC Compliance** which means a ton of deals are just waiting to be made.
- Pressure on MSP work to get cheaper. Compliance work is NOT a commodity, which means you can make **higher profit margins**
- **Competitive advantage** and economies of scale by specializing in a vertical
- **Serve and protect** our country by securing the Defense Industrial Base

If It's So Awesome – Why Isn't Everyone Doing It?

- Managing compliance across many different clients is hard
- Keeping track of status in compliance process
- Keeping track of all the compliance activity (that evidence is REQUIRED!)
- Getting them to actually listen to you
- Am I doing the right activity to get them to pass an assessment?
  - You don't feel like an "expert" – what business do you have doing this?
- Am I giving the right guidance to get them to pass an assessment?
  - Concerned about liability – what if you give the WRONG advice?
  - There are plenty of people who are happy to sell this stuff to them and give them BAD guidance and the WRONG products

How We Ended Up Needing To Figure Out CMMC

- Specialize in working with manufacturers
- Way back in 2016 we got wind of this thing called NIST 800-171
- Asked to learn it and speak to manufacturers about the requirement
- Hard to understand controls
- Pushback from clients to implement
- 100% failure rate of full implementation of controls
- Accountability required to assure implementation
- Clients desperately looking to US for help

But We Don't Know Anything About This "NIST Thing"

"RTFM" – Mark Cuban

(Read The Fucking Manual)

What Manual?

Every Single Doc We Could Get Our Hands On

- **DFARS 252.204-7012** - Safeguarding Covered Defense Information and Cyber Incident Reporting.
- **DFARS 252.204-7019** Notice of NISTSP 800-171 DoD Assessment Requirements.
- **DFARS 252.204-7020** NIST SP 800-171 DoD Assessment Requirements.
- **NIST SP 800-53** - Security and Privacy Controls for Information Systems and Organizations
- **NIST SP 800-171** - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- **NIST SP 800-171A** - Assessing Security Requirements for Controlled Unclassified Information
- **Referenced NIST SP's** (NIST 800-88, 800-37, 800-175B, many more…)
- **CMMC Model Overview, Scoping Guides, Self Assessment Guides**
- **Certified CMMC Professional Class and Field Guide**

Guess What We Discovered?

Requirements

- **FAR 52.204-21** - Basic Safeguarding of Covered Contractor Information Systems.
- **DFARS 252.204-7012** - Safeguarding Covered Defense Information and Cyber Incident Reporting.
- **DFARS 252.204-7019** - Notice of NIST SP 800-171 DoD Assessment Requirements.
- **DFARS 252.204-7020** - NIST SP 800-171DoD Assessment Requirements.
- **NIST SP 800-171** - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- **NIST SP 800-171A** - Assessing Security Requirements for Controlled Unclassified Information
- **False Claims Act (FCA)**, 31 U.S.C. §§ 3729 - 3733

Accept A Contract And Side Step Requirements?

- Subject to the False Claims Act
- https://www.justice.gov/civil/false-claims-act
- “Ensuring that citizens’ tax dollars are protected from fraud and abuse is among the department’s top priorities,” said Acting Assistant Attorney General Boynton. “The False Claims Act is one of the most important tools available to the department both to deter and to hold accountable those who seek to misuse public funds.”

Accept A Contract And Side Step Requirements?

- **Contractor fraud is a common type** of False Claims Act case. Whistleblowers can report contractors who defraud the government through bribes, kickbacks, or **false certifications of compliance** to win government contracts.
- **Defense contractor fraud is the most common type of contractor fraud.**
- Contract compliance violations like false certification of regulatory or statutory compliance also result in False Claims Act cases.

Show Up Guns Blazing?

- Not if you want to establish RAPPORT and CLOSE your sale

“Voss” Them: Use Tactical Empathy

- Voss refers to empathy as becoming utterly aware of the other person's perspective and understanding their viewpoints and emotions.
- In other words, tactical empathy is the act of **understanding another persons' mindset and feelings and making them feel understood.**
- *“Listening is a martial art, balancing the subtle behaviors of emotional intelligence and the assertive skills of influence, to gain access tot eh mind of another person.” – Chris Voss*

What Do They Say?

- “I don’t understand why I have to do this”
- “Its so expensive / I don’t know how I’m going to afford this”
- “I don’t trust what X is saying”
- “I already spent so much money/time/effort with X doing X, I don’t want this to happen again”

Establish Yourself As A Trusted Advisor

- Ego vs. Ego Strength
- Demonstrating industry and compliance knowledge
- Your NETWORK
- Solutions you have access to

So What Do You Charge?

- Decide what you are delivering:
  - Gap Assessments
  - POAM Management
  - Remediation
  - Documentation
  - GRC
  - Program Management
  - Security Toolsets
  - Training & Awareness / SecOps
  - MSP Services

So What Do You Charge?

- A CHECKLIST for compliance?
- Stuff? Are you delivering STUFF?
- OR ARE YOU DELIVERING VALUE?
- What's the difference?

“Stuff” vs. Value

- “Stuff”
  - Gap Assessments
  - POAM Management
  - Remediation
  - Documentation
  - GRC
  - Program Management
  - Security Toolsets
  - Training & Awareness / SecOps
  - MSP Services

“Stuff” vs. Value

- Value
  - *“Mature organizations create processes from regular projects”* – Nick Sonnenberg “Come Up For Air”
  - Do NOT deliver a checklist
  - Checklist approaches = poor organizational transformation and adoption + great costs
  - Implement a Cybersecurity Compliance Program for you that **identifies and reduces organizational risk**
  - You’re spending money and time: ***Is it in the right place?***
  - They are going to do the work anyway – **do a little more work and get 10x value**

You Can Price VALUE Higher

- ✓ When you bring value to a company – you can charge higher fees
- ✓ Price offering based on what you are able to deliver to your client

You Can Price VALUE Higher

- ✓ How much more?
- ✓ MSP Hourly Services = $150 - $250/hr
- ✓ Compliance Hourly Services = $200 - $350/hr
- ✓ …But that's not all you should think about…

You Can Price VALUE Higher

- ✓ Value your OWN time
- ✓ Think of your direct time investment being worth $500/hr - $1,000/hr
- ✓ **Why?**
- ✓ You will put in massive hours and effort to build a program template and system that every client will get the benefit from
- ✓ Don’t trade DOLLARS for HOURS – get paid based on the VALUE and measurable RESULTS you can bring to the organization

Use This Formula To Become A Sought-After CMMC Expert

- OSC's will know if they come to you, they would have a Proven Process
- Your leads will go from a few a MONTH to a bunch a WEEK
- Organizations will line up to co-market or create programs with you

Do NOT Try This Without A GRC Tool!

- Used to use spreadsheets – UGH sums that up
- You need a solid Governance Risk and Compliance Tool to store the progress and evidence of compliance
- I've personally demo-ed and tested dozens of tools
- Have not found a better fit than FutureFeed
- PS – FutureFeed is only getting better!

www.futurefeed.co

Get Plugged Into the CMMC Community

- LinkedIn
  - **Ryan Bonner:** https://www.linkedin.com/in/rybonner/
  - **Jacob Horne**: https://www.linkedin.com/in/jacob-evan-horne/
  - **Jim Goepel**: https://www.linkedin.com/in/james-goepel-gc-cto-cyber/
  - **Jeff Baldwin**: https://www.linkedin.com/in/drjeffbaldwin/
  - **Amira Armond**: https://www.linkedin.com/in/amira-armond-25a77a141/
  - **Joy Beland** - https://www.linkedin.com/in/joy-belinda-beland/
  - **Fernando Machado**: https://www.linkedin.com/in/fernando-machado-cissp-cism-cisa-ceh-5b5581124/
  - **Troy Fine:** https://www.linkedin.com/in/troyjfine/
  - **Matthew Titcombe**: https://www.linkedin.com/in/matthewtitcombe/
  - **Allison Giddens:** https://www.linkedin.com/in/allisongiddens/
  - **Ben Tchoubineh** - https://www.linkedin.com/in/ben-tchoubineh-2401113a/
  - **Mark Berman** - https://www.linkedin.com/in/markberman-ff/
  - **Matt Hoeper** - https://www.linkedin.com/in/mhoeper/
  - **Robert Metzger** - https://www.linkedin.com/in/robertmetzger/
  - **Eric Crusius** - https://www.linkedin.com/in/ericcrusius/
  - **Tony Buenger** - https://www.linkedin.com/in/tonybuenger/
  - **Tara Lemieux** - https://www.linkedin.com/in/tara-lemieux-4385781/

Get Plugged Into the CMMC Community

- CMMC-AB
  - Monthly Town Halls
  - Become an RP, RPA, CCP, or CCA
- Industry Working Groups
- Peer & Advisory Groups

Then There's The BANE Of Your Existence...

No, its not printers

Then There's The BANE Of Your Existence…

Documentation is required for compliance, but such a pain!

- Anywhere you see a **verb** in the controls = **documentation required**
- Assuring clients have the right docs – and **NOT just technical ones**
- If you like to write documentation, raise your hand!
- You want to just download something but most of the offerings for documentation are NOT functional. They look good on paper but are not usable in real life
- Writing them on your own takes 100's of hours
- We need simple, clear documentation to drive operations where we are in scope, and to provide to clients to assure they will pass assessments.

Don’t Worry

In a minute I’m going to show you the easy button to eliminate hundreds of hours creating documentation and a compliance program process into just minutes

We Had The Same Problem

How did we build it?

- Policies first
- Create Procedures or Processes
- Maybe throw in an IRP so something, cuz, requirements

It doesn't work

We Had The Same Problem

Flip the system

- Had procedures – tons of SOPs, because we are a process-driven MSP
- Created Plans as a collaborative way of managing clients
- Overarching Policies that are SIMPLE, RELEVANT and tie it all together

Ahhhhh…. Success! And its FUN now!

We Became A Sought-After CMMC Expert

- OSC's knew if they came to us, they would have a Proven Process
- Dubbed it the CMMC IT Documentation Toolkit Compliance Program
- Leads went from a few a MONTH to a few a WEEK
- Organizations lined up to co-market or create programs with us
- ***What's YOUR Proven Process?***

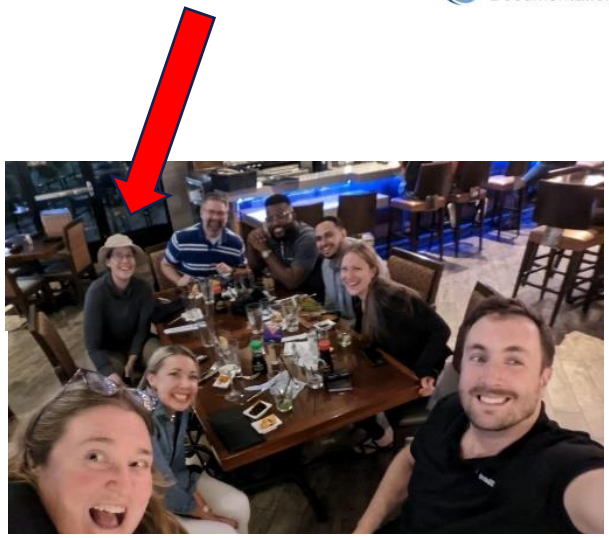
Ran It Past Smart People

Stacy Bostjanick, DoD CIO, CMMC Program
John Ellis, DIBCAC Director

"That's exactly what the DIB needs."

"Looks good! I'm going to send you a list of the evidence you'll need to collect so your clients are assessment-ready."

Fernando Machado, Cybersec
CMMC Assessor



"You are doing good work and deserve to be shouted out."

Amira Armond, Keiri Solutions
CMMC Assessor

The 5 Step Process Of A CMMC Compliance Program

1. Identify Key Data, Business Processes, and Technology
2. Validate Client's CMMC Self-Assessment
3. Create Discrete Projects To Close POAM
4. Onboard IT Documentation Toolkit CMMC Program
5. Implement Risk Management Plan & Meetings To Get & Stay Compliant

Risk Management As Mechanism For Getting & Staying Compliant

InTech SOLUTIONS

CMMC IT Documentation Toolkit

CompanyName

Ris

& F

The Risk Assessment will be both qua

Quarter 1

- Risks to organizational ope
- Prior Security Assessment
- Incident Reports
- Incident Response Testing
- Training & Awareness Plar
- Visitor and Network Room
- Asset Management Plan /
- Ticket Review: Request Tr
- Current threats and securi
- Security tool reports, audi
- Audit logging and analysis
- Onboarding, Transfer, and
- CUI media control and ma
- Removable Media List
- Change Management Proc
- Publicly Posted Informatio

Quarter 2

- Risks to organizational ope
- Prior Security Assessment
- Incident Reports
- Incident Response Testing

#ITNation

CMMC COMPLIANCE ACTIONS CADENCE

DAILY:

D

Tool Alerts Review

Review security and operational tools that have generated alerts, assess, and take action as necessary.

D

Backup Review

Verify backups have completed successfully and remediate any anomalies

WEEKLY:

Endpoint and Application Patching

Endpoints and Applications are patched on standard cadence.

Automated Maintenance

Automated maintenance is performed on Windows endpoints.

IT Security Tips Email

Cybersecurity awareness email tips are delivered to end user email boxes.

MONTHLY:

JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

Server Patching

Servers are patched monthly on a standard cadence.

JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

Simulated Phishing Exercises

Deploy simulated phishing exercise and analyze results for frequent clickers or other signs and/or anomalies.

JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

Firmware Patching

As new firmware patches become available, they are tested and applied monthly.

QUARTERLY:

Q1 Q2 Q3 Q4

Risk Management Meeting Process

Processes are followed from Risk Management Plan in preparation for RMT Meeting. Compliance is reported on. Remediation actions are created. POAM is updated with due dates. Self-Assessment is updated. Systems Security Plan is updated.

Q1 Q2 Q3 Q4

Assess Risks to Organizational Operations

Discuss risks to organization including mission, functions, image, or reputation, especially as related to being data custodians of FCI and CUI.

Q1 Q2 Q3 Q4

Security Assessment Review

Review annual Security Assessment findings for consideration of modifications to cybersecurity and compliance programs. Add any items that affect compliance to the POAM.

Q1 Q2 Q3 Q4

Incident Reports Review

Review past quarter incident reports to assure they were reported to DIBNET properly, if applicable. Consider if there are any mitigating actions that should be taken to avoid the incident from recurring.

Q1 Q2 Q3 Q4

Incident Response Tabletop Exercise

Perform tabletop exercise of the Disaster Recovery Business Continuity Plan or the Incident Response Plan.

Q1 Q2 Q3 Q4

Training & Awareness Plan Review

Review Training & Awareness Plan to assure it is up to date and on track. Create new plan for next year in Q4.

Q1 Q2 Q3 Q4

Physical Access Review

Review visitor and network room logs for any concerns, anomalies, and to assure the process to access the facility, physical CUI locations, and network room is being followed properly.

Q1 Q2 Q3 Q4

Asset Management Plan / IT Roadmap Review

Assure Asset lists are up to date, review lifecycling and budgeting, discuss considerations for IT projects, update on current and pending IT projects that affect compliance.

Q1 Q2 Q3 Q4

Ticket Review: Request Trends & Maintenance

Review request trends for any equipment, applications, or users that are impacting

Learn It, Replicate

- Learn how to create a compliance program
- Replicate the approach and apply to other compliance requirements and/or insurance requirements
- **That's why there are MSPs in our Toolkit Program who DO NOT OFFER CMMC COMPLIANCE AT ALL**

“Compliance Is Coming”
Are You Ready To Take Advantage Of The Opportunity?

Compliance is coming whether you're a government contractor, healthcare practice, or small business. I wanted to create a compliance program but **simply did NOT know where to begin**.

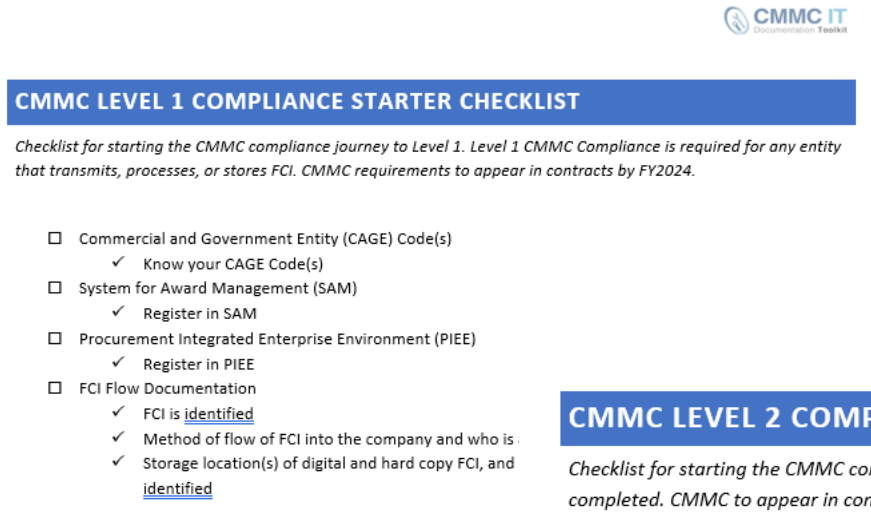
The **process and documentation** in the Toolkit alone are lightyears beyond anything else you are going to find.

The **weekly peer group** calls that allow you to share and compare your process with others who are also tackling this compliance gorilla, is a massive bonus

Ross Brouse,
Continuous Networks

FREE CHECKLISTS FROM TOOLKIT

- CMMC L1 Compliance
- CMMC L2 Compliance

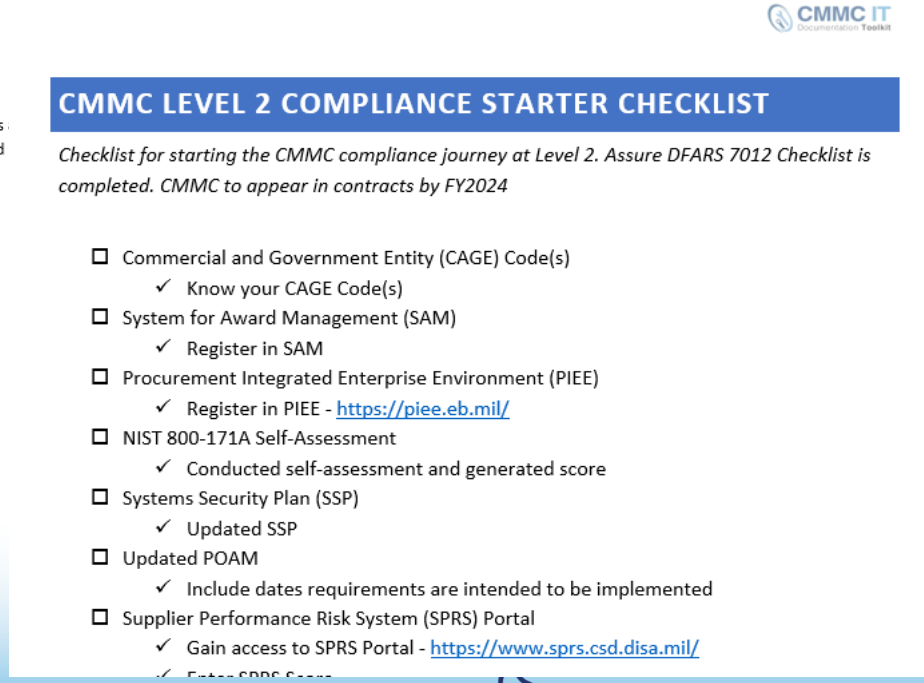


CMMC IT Documentation Toolkit

CMMC LEVEL 1 COMPLIANCE STARTER CHECKLIST

Checklist for starting the CMMC compliance journey to Level 1. Level 1 CMMC Compliance is required for any entity that transmits, processes, or stores FCI. CMMC requirements to appear in contracts by FY2024.

- ☐ Commercial and Government Entity (CAGE) Code(s)
  - ✓ Know your CAGE Code(s)
- ☐ System for Award Management (SAM)
  - ✓ Register in SAM
- ☐ Procurement Integrated Enterprise Environment (PIEE)
  - ✓ Register in PIEE
- ☐ FCI Flow Documentation
  - ✓ FCI is identified
  - ✓ Method of flow of FCI into the company and who is
  - ✓ Storage location(s) of digital and hard copy FCI, and identified



CMMC IT Documentation Toolkit

CMMC LEVEL 2 COMPLIANCE STARTER CHECKLIST

Checklist for starting the CMMC compliance journey at Level 2. Assure DFARS 7012 Checklist is completed. CMMC to appear in contracts by FY2024

- ☐ Commercial and Government Entity (CAGE) Code(s)
  - ✓ Know your CAGE Code(s)
- ☐ System for Award Management (SAM)
  - ✓ Register in SAM
- ☐ Procurement Integrated Enterprise Environment (PIEE)
  - ✓ Register in PIEE - https://piee.eb.mil/
- ☐ NIST 800-171A Self-Assessment
  - ✓ Conducted self-assessment and generated score
- ☐ Systems Security Plan (SSP)
  - ✓ Updated SSP
- ☐ Updated POAM
  - ✓ Include dates requirements are intended to be implemented
- ☐ Supplier Performance Risk System (SPRS) Portal
  - ✓ Gain access to SPRS Portal - https://www.sprs.csd.disa.mil/

EMAIL: info@intechit.net
"FREE STARTER CHECKLIST!"

QUESTIONS?

LINK WITH ME!

LinkedIn: www.linkedin.com/princessleia

Email: Leia@intechit.net

Signal: Leia Kupris Shilobod

Don't forget to fill out your

SESSION SURVEY