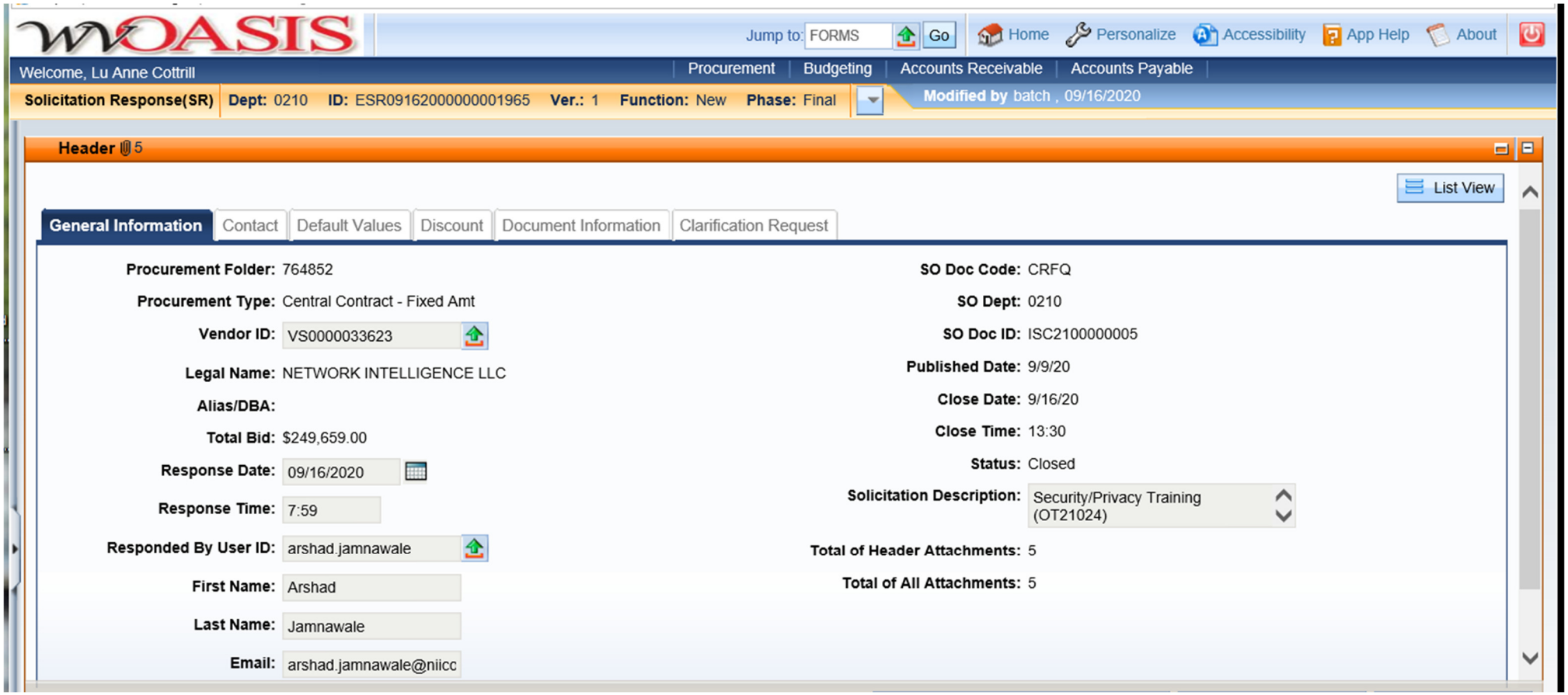
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.


wvOASIS
Jump to: FORMS Go
Home
Personalize
Accessibility
App Help
About
Welcome, Lu Anne Cottrill
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR) Dept: 0210 ID: ESR09162000000001965 Ver.: 1 Function: New Phase: Final
Modified by batch , 09/16/2020
Header 5
List View
General Information
Contact
Default Values
Discount
Document Information
Clarification Request
Procurement Folder: 764852
Procurement Type: Central Contract - Fixed Amt
Vendor ID: VS0000033623
Legal Name: NETWORK INTELLIGENCE LLC
Alias/DBA:
Total Bid: $249,659.00
Response Date: 09/16/2020
Response Time: 7:59
Responded By User ID: arshad.jamnawale
First Name: Arshad
Last Name: Jamnawale
Email: arshad.jamnawale@niicc
SO Doc Code: CRFQ
SO Dept: 0210
SO Doc ID: ISC2100000005
Published Date: 9/9/20
Close Date: 9/16/20
Close Time: 13:30
Status: Closed
Solicitation Description: Security/Privacy Training (OT21024)
Total of Header Attachments: 5
Total of All Attachments: 5

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder:	764852
Solicitation Description:	Security/Privacy Training (OT21024)
Proc Type:	Central Contract - Fixed Amt

Solicitation Closes	Solicitation Response	Version
2020-09-16 13:30	SR 0210 ESR09162000000001965	1

VENDOR

VS0000033623
NETWORK INTELLIGENCE LLC

Solicitation Number: CRFQ 0210 ISC2100000005

Total Bid: 249659 **Response Date:** 2020-09-16 **Response Time:** 07:59:38

Comments: Option 2 of our commercial proposal states
a) if we get lumpsum PO for 2 years then we can off discount of USD 17,500.00
b) if we get lumpsum PO for 3 years then we can off discount of USD 43,625.00
c) if we get lumpsum PO for 4 years then we can off discount of USD 89,659.00
we are open for further negotiation

FOR INFORMATION CONTACT THE BUYER
Jessica S Chambers
(304) 558-0246
jessica.s.chambers@wv.gov

Vendor Signature X **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Privacy and Cybersecurity Training Solution	1.00000	EA	50000.000000	50000.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments: Price Consist of LMS Portal for 25,000 users and Phishing simulation for 5,000 users, 5 scenario in a year. Hardware will be extra.

Extended Description:

Specification 3.1.1. Vendor must provide a Lump Sum Cost for Year One Contract Services.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Privacy and Cybersecurity Training Solution - Optional YR2	1.00000	EA	57500.000000	57500.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments: 200 USD per Hour extra for additional content apart form SOW

Extended Description:

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Two Contract Services.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Privacy and Cybersecurity Training Solution - Optional YR3	1.00000	EA	66125.000000	66125.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments: 200 USD per Hour extra for additional content apart form SOW

Extended Description:

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Three Contract Services.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Privacy and Cybersecurity Training Solution - Optional YR4	1.00000	EA	76034.000000	76034.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments: 200 USD per Hour extra for additional content apart form SOW

Extended Description:

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Four Contract Services.

NETWORK INTELLIGENCE
Global cybersecurity provider

Proposal
Security/Privacy Training from Network Intelligence, LLC.

Submitted to:

County Name

State of West Virginia

From

NETWORK INTELLIGENCE, LLC.

NETWORK
INTELLIGENCE
Global cybersecurity provider

NOTICE

This document contains information, which is the intellectual property of Network Intelligence, LLC. (hereinafter referred as NII). This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of Network Intelligence.

Nothing in this document constitutes a guaranty, warranty, or license, expressed or implied. Network Intelligence disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of Network Intelligence; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein and is advised to seek the advice of competent legal counsel, without obligation of Network Intelligence.

COPYRIGHT

TRADEMARKS

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

NETWORK INTELLIGENCE
Global cybersecurity provider

DOCUMENT SUBMISSION DETAILS

COMPANY	State of West Virginia
DOCUMENT TITLE	Proposal Security Privacy Training from Network Intelligence, LLC
DATE	16th Sept 2020
REF	Security Privacy Training / Security Training /NII/09092020
DOCUMENT TYPE	EXTERNAL

RECIPIENT DETAILS

NAME	Jessica S Chambers
Designation	Purchaser

DOCUMENT HISTORY

DATE	VERSION	AUTHOR	COMMENTS
16th Sept 2020	1.0	Arshad	Initial

NII CONTACT DETAILS

NAME	Arshad Jamnawale
TITLE	(Sr Sales & Marketing Manager)
COMPANY	Network Intelligence, LLC.
ADDRESS	16192 Costal Highway, Lewes, Delaware – 19958, Country of Sussex.
CELL PHONE NO.	+91 887 974 5450
EMAIL ADDRESS	arshad.jamnawale@niiconsulting.com
WEBSITE	www.niiconsulting.com

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

CONTENTS

1. EXECUTIVE SUMMARY 6

1.1 BACKGROUND OF ENGAGEMENT 6
1.2 ENGAGEMENT BENEFITS DELIVERED 6

2. SCOPE OF WORK: 7

3. DELIVERABLES 10

4. COMMERCIAL OFFERINGS 13

4.1 TERMS AND CONDUCTIONS 15

5. ABOUT NETWORK INTELLIGENCE, LLC. 16

6. ABOUT INSTITUTE OF INFORMATION SECURITY 17

6.1. TOP REASON TO CHOOSE INSTITUTE OF INFORMATION SECURITY 17

6.1.1. LATEST TECHNOLOGY COVERAGE 17

6.1.2. CYBERSECURITY INDUSTRY ALIGNMENT 17

6.1.3. EMPHASIS ON HANDS-ON PRACTICAL 17

6.1.4. FLEXIBLE DELIVERY MODELS 17

6.1.5. PIONEERS OF INFORMATION SECURITY TRAININGS 17

6.2. TRAINING EXPERTISE 18

6.3. EXTENSIVE CONSULTING EXPERIENCE 18

6.4. SUBJECT MATTER EXPERTISE 18

6.5. COMPREHENSIVE KNOWLEDGE-TRANSFER 18

6.6. COMMITMENT TO SECURITY RESEARCH 19

6.7. INTERNATIONAL AND DOMESTIC ACCREDITATION.....20

6.8. CUSTOMIZED COURSES 20

6.9. OUR CLIENTS (TRAINING CLIENTS IN INDIA) 20

7. SAMPLE LMS PORTAL.....25

1. EXECUTIVE SUMMARY

West Virginia was Incorporated in 1935 by Circuit Court. Named for New Haven, Connecticut, the home city of the owners of the first coal mine opened at that place. Formerly known as New London. Population, 1559; elections held every two years on the first Tuesday in June; officials take office July first.

Network Intelligence through its deep domain expertise in Penetration Testing and exposure to Global Cybersecurity Frameworks, **Cybersecurity Trainings** & best Practices bring to the table the highest quality of Resources and Project Management expertise to Execute the Scope as defined in the RFP.

1.1 BACKGROUND OF ENGAGEMENT

Customized cybersecurity and privacy training that is hosted in a vendor-managed learning management system (LMS). Seeking a product that will provide security and privacy training for an estimated 25,000 end users with an integrated phishing simulator and training.

1.2 ENGAGEMENT BENEFITS DELIVERED

NII is keen to provide Digital Learning Platform for West Virginia based on the below Scope mentioned. We would like to ensure that the provided Digital Learning Platform will be customized and we will also ensure that all the below mentioned trainings are embedded in our Digital Learning Platform for West Virginia.

2. SCOPE OF WORK:

1.1 PURPOSE AND SCOPE:

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish a contract for the purchase of Cybersecurity and Privacy Training That is hosted in a vendor managed Learning Management System (LMS). The WVPT is seeking a product that will provide security and privacy training for an estimated 25,000 end-users what an integrated Phishing Simulator and training.

2.1 GENERAL REQUIREMENT

3.1. Mandatory Contract Item Requirements: The contract item is meeting the mandatory requirements listed below.

3.1.1. Custom Privacy and Cyber Security Training Solution

3.1.1.1. The Privacy and Cyber Security Training Solution is an adaptive curriculum for Cybersecurity (Information Security) and Privacy Training. The State of West Virginian can customize the training topics.

3.1.1.2. The Privacy and Cybersecurity Training Solution can be integrated with the State current Active Directory Environment.

3.1.1.3. The Privacy and Cybersecurity Training Solution does have editable modules for the following Topics

- 3.1.1.3.1. Understanding Security Threats
- 3.1.1.3.2. Security Responsibility
- 3.1.1.3.3. Physical Threat
- 3.1.1.3.4. Emergency Preparation
- 3.1.1.3.5. Securing Work Areas and Resources
- 3.1.1.3.6. Access Control
- 3.1.1.3.7. Safe Computing and Electronic Threats
- 3.1.1.3.8. Social Engineering Threats
- 3.1.1.3.9. Password Guidelines
- 3.1.1.3.10. Safe Remote and Mobile Computing
- 3.1.1.3.11. Acceptable Use
- 3.1.1.3.12. Phishing Identification and Prevention
- 3.1.1.3.13. Physical Security and Emergency Preparation
- 3.1.1.3.14. Responsible Social Networking
- 3.1.1.3.15. Protecting and Handling Data
- 3.1.1.3.16. Records Management and Data Classification
- 3.1.1.3.17. Privacy Awareness and Privacy Principles (PII)
- 3.1.1.3.18. Complying with PCI DSS
- 3.1.1.3.19. Complying with HIPAA
- 3.1.1.3.20. Understanding PII
- 3.1.1.3.21. Social Engineering

3.1.1.3.22. Identity Theft
3.1.1.3.23. Incident Reporting
3.1.1.3.24. HIPAA Training, Includes
3.1.1.3.24.1. What is HIPAA?
3.1.1.3.24.2. Personal Health Identifying Information
3.1.1.3.24.3. Covered Entities
3.1.1.3.24.4. HIPAA Privacy Rule
3.1.1.3.24.5. HIPPA Security Rule
3.1.1.3.24.6. HIPPA Enforcement Rule
3.1.1.3.24.7. HIPAA Breach Notification Rule
3.1.1.3.24.8. The Importance of Confidentiality
3.1.1.3.24.9. The Minimum Necessary Standard
3.1.1.3.24.10. Business Associate Agreement
3.1.1.3.24.11. Patient Rights

3.1.1.4. The Privacy and Cybersecurity Training Solution allows the option to include Role-Based Training
3.1.1.5. The Privacy and Cybersecurity Training Solution Supports 25,000 active employees and On-site contractors.
3.1.1.6. The Privacy and Cybersecurity Training Solution can be hosted in LMS that is Compatible with a SCOEM 2.0 or higher
3.1.1.7. LMS can allow for additional 3rd party SCORM compliant courses to be uploaded
3.1.1.8. LMS can Integrate with Microsoft Lightweight Directory Access Protocol (LDAP)
3.1.1.9. The Privacy and Cybersecurity Training Solution can be branded with the West Virginia State and Office of Technology Logos.
3.1.1.10. The Privacy and Cybersecurity Training Solution contains appropriate Images to the training content and content West Virginia specific graphics.
3.1.1.11. The Privacy and Cybersecurity Training Solution contains Customer-Customizable “Resource” section
3.1.1.12. The Privacy and Cybersecurity Training Solution can generate optional Certificates of Completion
3.1.1.13. The Privacy and Cybersecurity Training Solution can provide options for course rollout assistance, Specifically;

3.1.1.13.1.1. Launching an entire course
3.1.1.13.1.2. Launching sections for a course
3.1.1.13.1.3. Nothing students as “passed” or “failed”
3.1.1.13.1.4. Pass or Failed percentage or score can be customizable

3.1.1.14. The Privacy and Cybersecurity Training Solution can allow knowledge check and graded assessments
3.1.1.15. The Privacy and Cybersecurity Training Solution do have a targeted length of at least 30 minutes, and no more than 45 minutes, of education content.
3.1.1.16. The Privacy and Cybersecurity Training Solution do provide a phishing simulator along with training if an end-user fails the phishing simulation.

3.1.1.17. The Phishing simulator does have predesigned and editable phishing templates for users conducting the simulation.

- 3.1.1.17.1.1. Customization can be included for the email message itself along with; attachments and web address the end user will click on
- 3.1.1.17.1.2. Predesigned templates do mimic current real-world phishing attacks.

3.1.1.18. The phishing simulator supports multifactor authentication for log-in.

3.1.1.19. The phishing simulator can be integrated with Microsoft Lightweight Directory Access Protocol (LDAP)

3.1.1.20. Can provide reports, visualization and graphics showing user interactions.

- 3.1.1.20.1.1. Reports can be exported to popular file formats for distribution such as .pdf .csv .xlsx etc.
- 3.1.1.20.1.2. Reports can generate reports for specific end-user or specific state.

3.1.1.21. The phishing simulator support automation for creating future tests and automatically launches them on the specified date.

3.1.1.22. The phishing simulator can also include a reporting option for the end-user to report phishing emails and track the reporting statistics for testing campaigns.

- 3.1.1.22.1.1. The reporting option can be utilized for all phishing emails reported to the Office of Technology.
- 3.1.1.22.1.2. All tools and processes that are utilized to analyze malicious emails with the reporting tool.

3.1.1.23. The phishing simulator can test for user input (i.e. The user clicks on the link and provides request information to “scammers”)

3.1.1.24. The phishing simulator supports attachments.

3.1.1.25. The simulator can provide, at minimum statistics on the user that clicked links and/or visited sites, provided credentials, opened or forwarded the email, time stamps for interactions, phishing training, and test results

3.1.1.26. The phishing simulator supports phishing campaigns up to 5,000 users/email addresses.

3.1.1.27. The phishing simulator owns an end-user education option in the form of an educational landing page, reply email, or training module.

3. DELIVERABLES

1.1. PURPOSE AND SCOPE:

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish a contract for the purchase of Cybersecurity and Privacy Training That is hosted in a vendor managed Learning Management System (LMS). The WVPT is seeking a product that will provide security and privacy training for an estimated 25,000 end-users what an integrated Phishing Simulator and training.

1.2. GENERAL REQUIREMENT

1.3. Mandatory Contract Item Requirements: The contract item is meeting the mandatory requirements listed below.

1.3.1. Custom Privacy and Cyber Security Training Solution

1.3.1.1. The Privacy and Cyber Security Training Solution is an adaptive curriculum for Cybersecurity (Information Security) and Privacy Training. The State of West Virginian can customize the training topics.

1.3.1.2. The Privacy and Cybersecurity Training Solution can be integrated with the State current Active Directory Environment.

1.3.1.3. The Privacy and Cybersecurity Training Solution does have editable modules for the following Topics

- 1.3.1.3.1. Understanding Security Threats
- 1.3.1.3.2. Security Responsibility
- 1.3.1.3.3. Physical Threat
- 1.3.1.3.4. Emergency Preparation
- 1.3.1.3.5. Securing Work Areas and Resources
- 1.3.1.3.6. Access Control
- 1.3.1.3.7. Safe Computing and Electronic Threats
- 1.3.1.3.8. Social Engineering Threats
- 1.3.1.3.9. Password Guidelines
- 1.3.1.3.10. Safe Remote and Mobile Computing
- 1.3.1.3.11. Acceptable Use
- 1.3.1.3.12. Phishing Identification and Prevention
- 1.3.1.3.13. Physical Security and Emergency Preparation
- 1.3.1.3.14. Responsible Social Networking
- 1.3.1.3.15. Protecting and Handling Data
- 1.3.1.3.16. Records Management and Data Classification
- 1.3.1.3.17. Privacy Awareness and Privacy Principles (PII)
- 1.3.1.3.18. Complying with PCI DSS
- 1.3.1.3.19. Complying with HIPAA
- 1.3.1.3.20. Understanding PII
- 1.3.1.3.21. Social Engineering

1.3.1.3.22. Identity Theft
1.3.1.3.23. Incident Reporting
1.3.1.3.24. HIPAA Training, Includes
1.3.1.3.24.1. What is HIPAA?
1.3.1.3.24.2. Personal Health Identifying Information
1.3.1.3.24.3. Covered Entities
1.3.1.3.24.4. HIPAA Privacy Rule
1.3.1.3.24.5. HIPPA Security Rule
1.3.1.3.24.6. HIPPA Enforcement Rule
1.3.1.3.24.7. HIPAA Breach Notification Rule
1.3.1.3.24.8. The Importance of Confidentiality
1.3.1.3.24.9. The Minimum Necessary Standard
1.3.1.3.24.10. Business Associate Agreement
1.3.1.3.24.11. Patient Rights

1.3.1.4. The Privacy and Cybersecurity Training Solution allows the option to include Role-Based Training
1.3.1.5. The Privacy and Cybersecurity Training Solution Supports 25,000 active employees and On-site contractors.
1.3.1.6. The Privacy and Cybersecurity Training Solution can be hosted in LMS that is Compatible with a SCOEM 2.0 or higher
1.3.1.7. LMS can allow for additional 3rd party SCORM compliant courses to be uploaded
1.3.1.8. LMS can Integrate with Microsoft Lightweight Directory Access Protocol (LDAP)
1.3.1.9. The Privacy and Cybersecurity Training Solution can be branded with the West Virginia State and Office of Technology Logos.
1.3.1.10. The Privacy and Cybersecurity Training Solution contains appropriate Images to the training content and content West Virginia specific graphics.
1.3.1.11. The Privacy and Cybersecurity Training Solution contains Customer-Customizable “Resource” section
1.3.1.12. The Privacy and Cybersecurity Training Solution can generate optional Certificates of Completion
1.3.1.13. The Privacy and Cybersecurity Training Solution can provide options for course rollout assistance, Specifically;

1.3.1.13.1.1. Launching an entire course
1.3.1.13.1.2. Launching sections for a course
1.3.1.13.1.3. Nothing students as “passed” or “failed”
1.3.1.13.1.4. Pass or Failed percentage or score can be customizable

1.3.1.14. The Privacy and Cybersecurity Training Solution can allow knowledge check and graded assessments
1.3.1.15. The Privacy and Cybersecurity Training Solution do have a targeted length of at least 30 minutes, and no more than 45 minutes, of education content.
1.3.1.16. The Privacy and Cybersecurity Training Solution do provide a phishing simulator along with training if an end-user fails the phishing simulation.

1.3.1.17. The Phishing simulator does have predesigned and editable phishing templates for users conducting the simulation.

1.3.1.17.1.1. Customization can be included for the email message itself along with; attachments and web address the end user will click on

1.3.1.17.1.2. Predesigned templates do mimic current real-world phishing attacks.

1.3.1.18. The phishing simulator supports multifactor authentication for log-in.

1.3.1.19. The phishing simulator can be integrated with Microsoft Lightweight Directory Access Protocol (LDAP)

1.3.1.20. Can provide reports, visualization and graphics showing user interactions.

1.3.1.20.1.1. Reports can be exported to popular file formats for distribution such as .pdf .csv .xlsx etc.

1.3.1.20.1.2. Reports can generate reports for specific end-user or specific state.

1.3.1.21. The phishing simulator support automation for creating future tests and automatically launches them on the specified date.

1.3.1.22. The phishing simulator can also include a reporting option for the end-user to report phishing emails and track the reporting statistics for testing campaigns.

1.3.1.22.1.1. The reporting option can be utilized for all phishing emails reported to the Office of Technology.

1.3.1.22.1.2. All tools and processes that are utilized to analyze malicious emails with the reporting tool.

1.3.1.23. The phishing simulator can test for user input (i.e. The user clicks on the link and provides request information to “scammers”)

1.3.1.24. The phishing simulator supports attachments.

1.3.1.25. The simulator can provide, at minimum statistics on the user that clicked links and/or visited sites, provided credentials, opened or forwarded the email, time stamps for interactions, phishing training, and test results

1.3.1.26. The phishing simulator supports phishing campaigns up to 5,000 users/email addresses.

1.3.1.27. The phishing simulator owns an end-user education option in the form of an educational landing page, reply email, or training module.

We request you to refer <u>Section 7</u> for look and feel of our LMS portal we can customise as per West Virginia Requirement

4. COMMERCIAL OFFERINGS

4.1 COMMERCIALS AS PER WEST VIRGINIA (OPTION 1)

Lump Sum Cost for Year One Contract Service

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
01	Security/Privacy Training Solution With Considering 5 Scenarios for Phishing simulation in a year	1	1	USD 50,000.00	**USD 50,000.00**

Lump Sum Cost for Year Two Contract Service

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
02	Security/Privacy Training Solution – Only Maintenance of the LMS **(with no change in content)**	1	1	USD 57,500.00	**USD 57,500.00**

Assuming change in the content of Training, Value will be defined as per the Scope and content of the Training, we will charge USD 200/- per hour for revising the content.

Lump Sum Cost for Year Three Contract Service

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
03	Security/Privacy Training Solution – Only Maintenance of the LMS **(with no change in content)**	1	1	USD 66,125.00	**USD 66,125.00**

Assuming change in the content of Training, Value will be defined as per the Scope and content of the Training, we will charge USD 200/- per hour for revising the content.

Lump Sum Cost for Year Four Contract Service

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
04	Security/Privacy Training Solution – Only Maintenance of the LMS **(with no change in content)**	1	1	USD 76,043.00	**USD 76,034.00**

Assuming change in the content of Training, Value will be defined as per the Scope and content of the Training, we will charge USD 200/- per hour for revising the content.

All Deliverables will be executed offsite.

4.2 Option 2 (Commercial with LumpSum PO for Multiple Years)

Lump Sum Cost for One Year Contract Service with One Year PO

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
01	Security/Privacy Training Solution With Considering 5 Scenarios for Phishing simulation in a year	1	1	USD 50,000.00	**USD 50,000.00**

Lump Sum Cost for Two Years Contract Service with Two Year PO

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
01	Security/Privacy Training Solution With Considering 5 Scenarios for Phishing simulation in a year **(with no change in content)**	1	1	USD 90,000.00	**USD 90,000.00**

Lump Sum Cost for Three Years Contract Service with Three Year PO

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
01	Security/Privacy Training Solution With Considering 5 Scenarios for Phishing simulation in a year **(with no change in content)**	1	1	USD 130,000.00	**USD 130,000.00**

Lump Sum Cost for Four Years Contract Service with Four Year PO

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
01	Security/Privacy Training Solution With Considering 5 Scenarios for Phishing simulation in a year **(with no change in content)**	1	1	USD 160,000.00	**USD 160,000.00**

4.3 TERMS AND CONDUCTIONS

a. Taxes will be extra,
b. **Note** above is per year pricing or individual years, assuming POs will be released per Year – Option 1
c. **Note** above is not per year pricing but consolidated pricing for all 2 or 3 or 4 years for Option 2
d. Payment terms will be 50% Advance, 40% on Content delivery and 10% on Handover of LMS to customer
e. Post-handover, any addition of content post one year we will be charging USD 200 per hour for any additional content development as per the Scope that will be defined in future.
f. Invoice of these additional Scope will be raised post completion of activity.
g. For Year 2, Year 3 and Year 4 Payment terms will be quarterly advance for LMS.
h. If hardware required that must be provided by the client

5. ABOUT NETWORK INTELLIGENCE, LLC.

Network Intelligence, incorporated in 2001, is a committed and well-recognized provider of **services**, **solutions** and **products** in the IT Governance, **Risk Management**, and **Compliance** space. Our professionals have made a mark for themselves with highly satisfied clients across the globe supported by our offices in India and the Middle East. As an ISO 27001-certified company ourselves, we are strongly positioned to understand your needs and deliver the right answers to your security and compliance requirements. We have won accolades at numerous national and international forums and conferences. Our work truly speaks for itself and our **clients** are the strongest **testimony** to the quality of our services!

6. ABOUT INSTITUTE OF INFORMATION SECURITY

The Institute of Information Security (**Training Division of Network Intelligence India Pvt. Ltd., DBA CAPL in Mumbai, India**) is one of the most trusted sources of hands-on trainings in information security, providing excellent unmatched practical training to individuals and corporates around the globe for over a decade. With the backing of our brilliant technical team providing consulting services for the past 18 years under the brand name of Network Intelligence, we are here to train, mentor and support your career in cybersecurity. Our emphasis on hands-on practical training gives our clients and students an edge to grow rapidly and advance professionally in their respective career(s).

We have put together a panel of brilliant trainers who have many years of experience in the exciting field of information security.

Keeping in mind the requirements of the industry our training programs are designed to prepare the candidates/professionals attending our trainings to meet the challenges they will be facing in real life situations.

6.1. TOP REASON TO CHOOSE INSTITUTE OF INFORMATION SECURITY

6.1.1. LATEST TECHNOLOGY COVERAGE

Be it cloud security or IoT security or the use of Big Data for Security Analytics, our training programs are always being updated to cover the latest trends in cybersecurity

6.1.2. CYBERSECURITY INDUSTRY ALIGNMENT

Our training programs are developed and vetted by hands-on practitioners who ensure that the content is closely aligned to the market needs of the cybersecurity industry

6.1.3. EMPHASIS ON HANDS-ON PRACTICAL

Across all our courses, more than 60% of time is spent on practical hands-on activities designed to help participants get confidence via assignments, hands-on exercises and labs that simulate real-world scenarios

6.1.4. FLEXIBLE DELIVERY MODELS

Our trainings are available as standard courses delivered at our various branches, as well as customized programs that can be delivered on-premises or virtually.

6.1.5. PIONEERS OF INFORMATION SECURITY TRAININGS

The USP of all our trainings is the hands-on that we provide, our focus is on real-life practical knowledge sharing, and not tool-based PPT slides. All our trainings are conducted by highly experienced practitioners who are dyed-in-the-wool penetration testers. The material is cutting edge and updated with even the most recent developments in information security.

6.2. TRAINING EXPERTISE

Our company has been training professionals from various companies for over three years now. The essential elements of our training workshops are:

- Not just PowerPoint presentations. Our workshops include a very heavy emphasis on hands-on practice. Every subject is covered below ends with a hands-on exercise
- Sincere efforts towards Knowledge Transfer. Our trainers will give you the complete knowledge they possess in terms of tools, techniques, and resources.
- Strong grasp of technical fundamentals. As the next few sections will show, our trainers have tremendous grasp of the technical details of the security of various technologies. We keep ourselves abreast of the latest developments and are always on the cutting-edge of security.
- Repeat clients. Companies such as BNP Paribas, HSBC, State Bank of India, Reserve Bank of India, BPCL, and many others are regular participants of our training workshops.
- Continuously improving methodology executed by a team of experienced trainers

6.3. EXTENSIVE CONSULTING EXPERIENCE

We (Network Intelligence, LLC. & Network Intelligence India Pvt. Ltd.) have provided the profiles of the consultants who will be engaged in this assignment. They are highly certified as well as experienced in network and security audits. Some of the pertinent certifications are:

- Certified Information Systems Security Professionals (CISSP)
- Certified Information Systems Auditors (CISA)
- Certified Information Security Managers (CISM)
- BS 25999 Lead Auditor (Business Continuity Management)
- ISO 27001 Lead Auditor and Implementer
- Certified Ethical Hackers (CEH)
- Cisco Certified Network Associate (CCNA)
- Microsoft Certified Systems Engineer (MCSE)

6.4. SUBJECT MATTER EXPERTISE

Our trainers are subject matter experts and possess practical knowledge of security issues faced by different organizations. Our trainers have worked on all platforms including mainframes and OpenVMS

6.5. COMPREHENSIVE KNOWLEDGE-TRANSFER

In all our training exercises, be it part of an ISO 27001 implementation or an in-house workshop, our over-riding objective is complete and comprehensive knowledge transfer to our participants. We lay maximum emphasis on practical hands-on training and believe that only by actually practicing the precepts can they be learnt best.

6.6. COMMITMENT TO SECURITY RESEARCH

Our teams are constantly engaged in extensive research covering various aspects of information security and penetration testing. The results from these efforts have been well-received by the security community; some of these are listed below:

We are one of the few companies actively engaged in security research. Here are some significant research results:

- Books: 'Linux Security, Audit and Controls', an ISACA publication. For details, visit here
- Articles: Articles published at ISACA, Security Focus, and the Institute for Internal Auditors.
- Presentations: We have been invited speakers at international conferences such asBlack hat, IT Underground, Interop and IIT security conferences.
- Advisories: We have found security vulnerabilities in products from vendors such as Oracle, Microsoft, Macromedia,

6.7. INTERNATIONAL AND DOMESTIC ACCREDITATION

Our consulting arm, NII, is one of the first Information Security consulting firms to have achieved the ISO/IEC 27001 certification. The scope of our certification covers all our services, and ensures secure transmission, storage and disposal of all client confidential information. Our consulting arm, NII is also empanelled as a security auditor by the CERT-In, the Indian Computer Emergency Response Team, an initiative of the Government of India. NII is also registered with the United Nations Global Marketplace, as an accepted vendor to UN organizations such as WFP, FAO, UNESCO, etc.

6.8. CUSTOMIZED COURSES

We have a standard set of courses outlined in different information security domains. However, we also customize the training according to the clients' requirements.

6.9. OUR CLIENTS (TRAINING CLIENTS GLOBALLY)

Accelya Kale	Integreon Managed Solutions
Adobe Systems	Intellectus Knowledge Management
Alcriti	Intertek
Amdocs	ISACA Mumbai Chapter
Angelique International Limited	ITC -Ltd-Hotels Divisions
Arab National Bank	Ivy Tech
Asia Society for Social Improvement	JM Financial Ltd
Assist ASIA SOCIETY	KEC International Limited
Atos India Pvt Ltd	King Abdulaziz City for Science and Technology
AXA Bussiness Services	Kotak Mahindra Bank Limited

Axis Bank Ltd	KPMG Limited
Axis Risk Consulting Service Pvt. Ltd.	K-Secure
Bajaj Allianz	L & T Technology Services
Bajaj Auto Finance Ltd.	Mahindra SSG
Bank of Baroda	MGage India Pvt ltd
Bank Of India	Microsoft Corp India Ltd
Bharat Petroleum Learning Centre	Nabard
Bharti Airtel Ltd	Nabil Bank Limited
Bhartiya Samruddhi Finance Ltd	Netmagic Solutions Pvt Ltd
Birla Global Finance Company Limited	Nomura
BNP Paribas	NSDL Technology
BPCL	Null
Canara Bank	Pentair Thermal Mgt Pvt Ltd
Capgemini	Pragati Software Pvt Ltd
Capita India Pvt Ltd	Principal Global Services

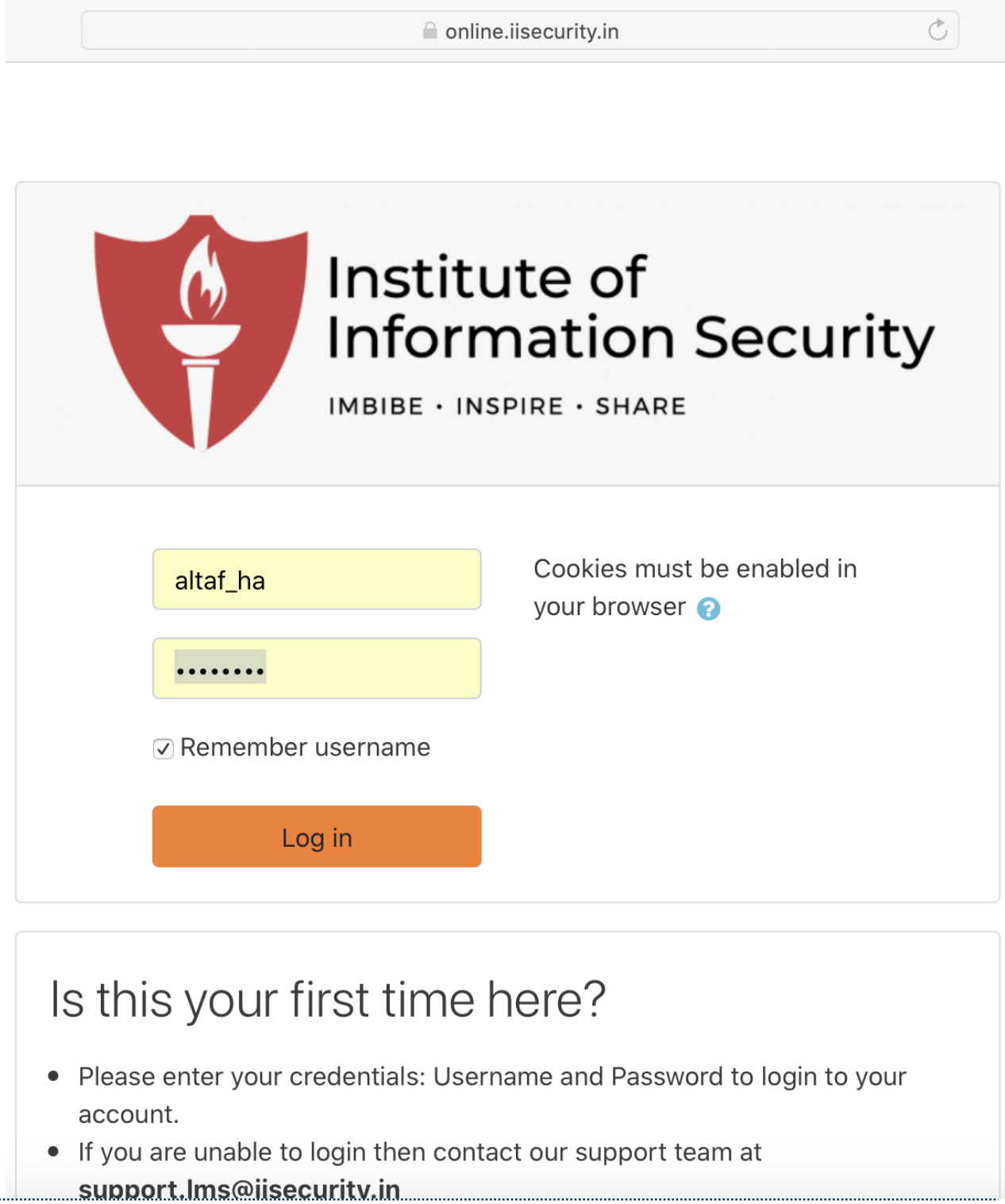
CDAC	Reliance Infocomm
Citigroup	Reserve Bank of India
CMS Computers	Royal Group
Computer Society of India	RSAM technologies India Pvt ltd
Credit Analysis & Research Ltd	R-Systems International Limited
Datamatics Global Services Ltd	Sahara India Finance Corporation Ltd
Defence Research & Development Organization (DRDO)	Samba FInancial group
Delhi International Airport Private Ltd.	Saraswat Co-Operative
Digital Jewels	Sarvanan- QlikTech India Privated Limited
Eclerx Services Ltd	Secure Matrix (India) Pvt. Ltd.
Ernst & Young, Qatar	Sharekhan
Essar	SIDBI
EXL Services	Sierra-Cedar
E-Zest Solutions Pvt Ltd	Society for Integrated Circuit Technology

Financial Software and Systems (I) Ltd.	SS&C Globe OP
FINO	Standard Chartered
FIS	State Bank of India
GCO Technology Center	Suma Soft
Genesis Software	Symantec
GEP solutions	Tata AIG
Global Landmark Media	Tata Communications Pvt ltd
Globant	Tata Interactive Systems
GMR Hyderabad International Airport Pvt. Ltd.	Tata Motors Ltd
Green Peace India	The Kalyan Janata Sahakari Bank Ltd.
Gulf International Bank	The National Electronics (Riyadh)
Haya Water	Trigyn Technologies Ltd
HDFC bank	University of Zambia
Holcim Services (South Asia) Limited	Unza Computer Centre
Honeywell	UPL Limited

HPCL	Venture Infotek
HSBC	Vital Health Care
HSBC Software	Vodafone
Huntsman	VSNL
ICICI Bank Limited	Wipro
ICICI Prudential Asset Management	WNS Global Services
ICICI Prudential Life Insurance Co. Ltd.	Worldline
IDFC Bank	Yes Bank Ltd
I-Flex Solutions	ZenQ
IGEFI Software India Pvt. Ltd	Infoserve
Indo German Institute of Advanced Technology	Infosys Limited
IndusInd Bank Ltd	Integrated Learning Solutions
Information Technology and Management Institute	

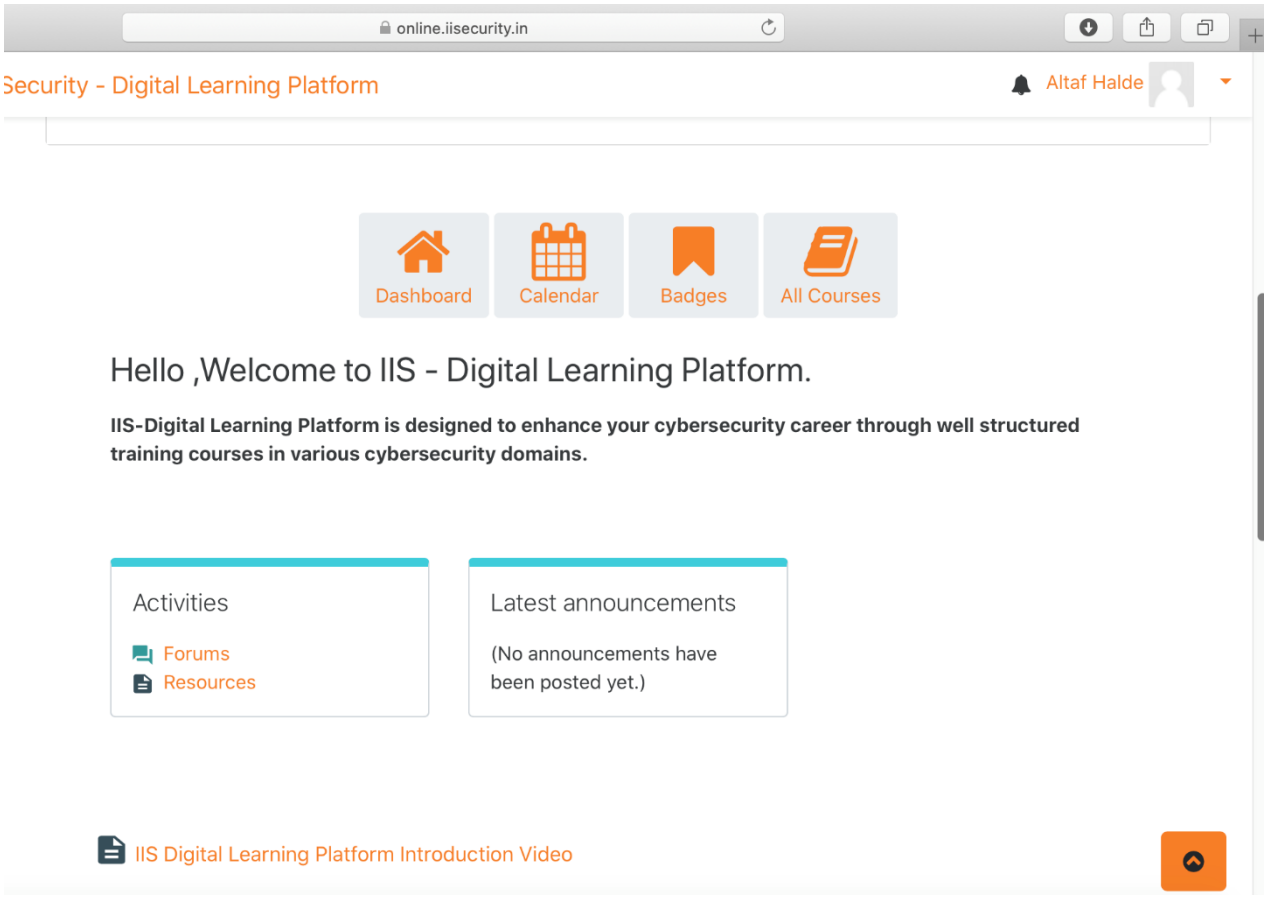
7. SAMPLE LMS PORTAL

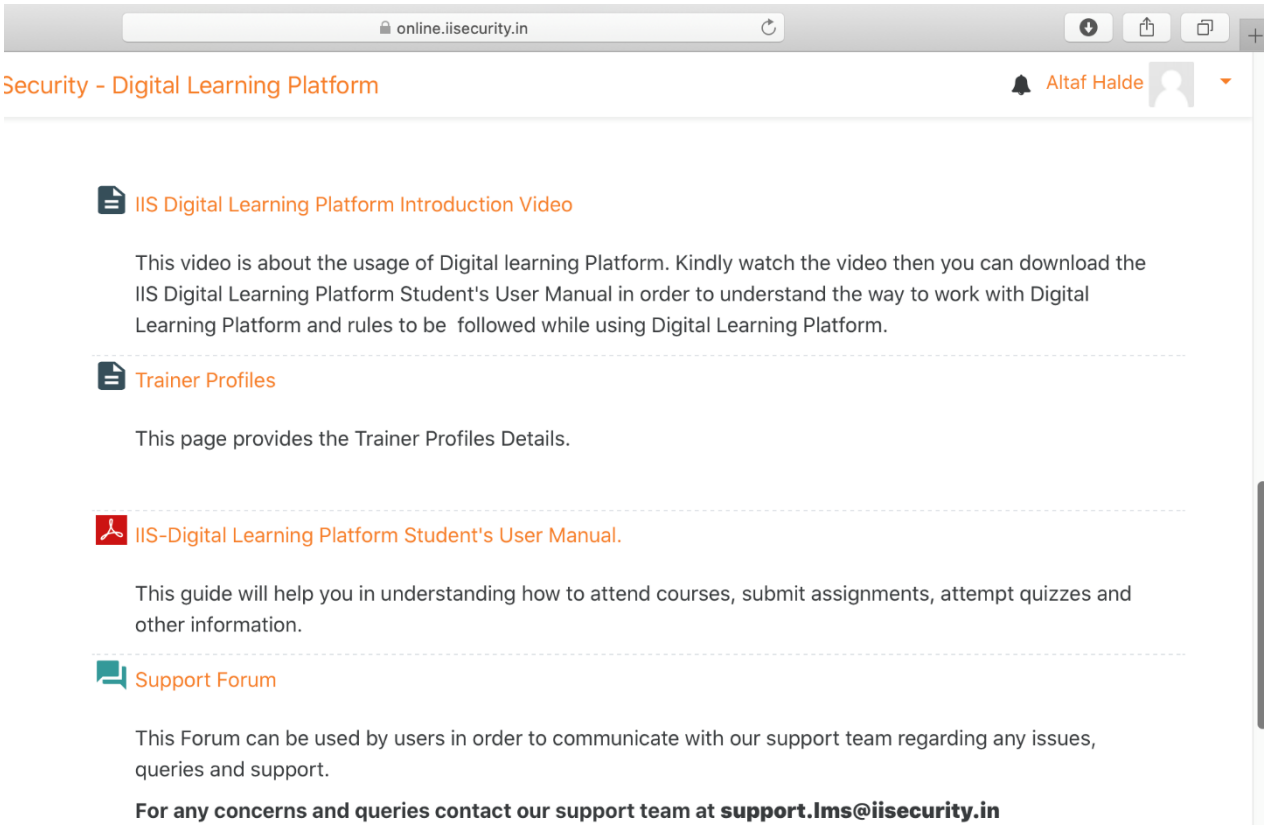
We are glad to share you Look and Feel of the LMS Portal, we are even glad to show Demo to give demo for same.

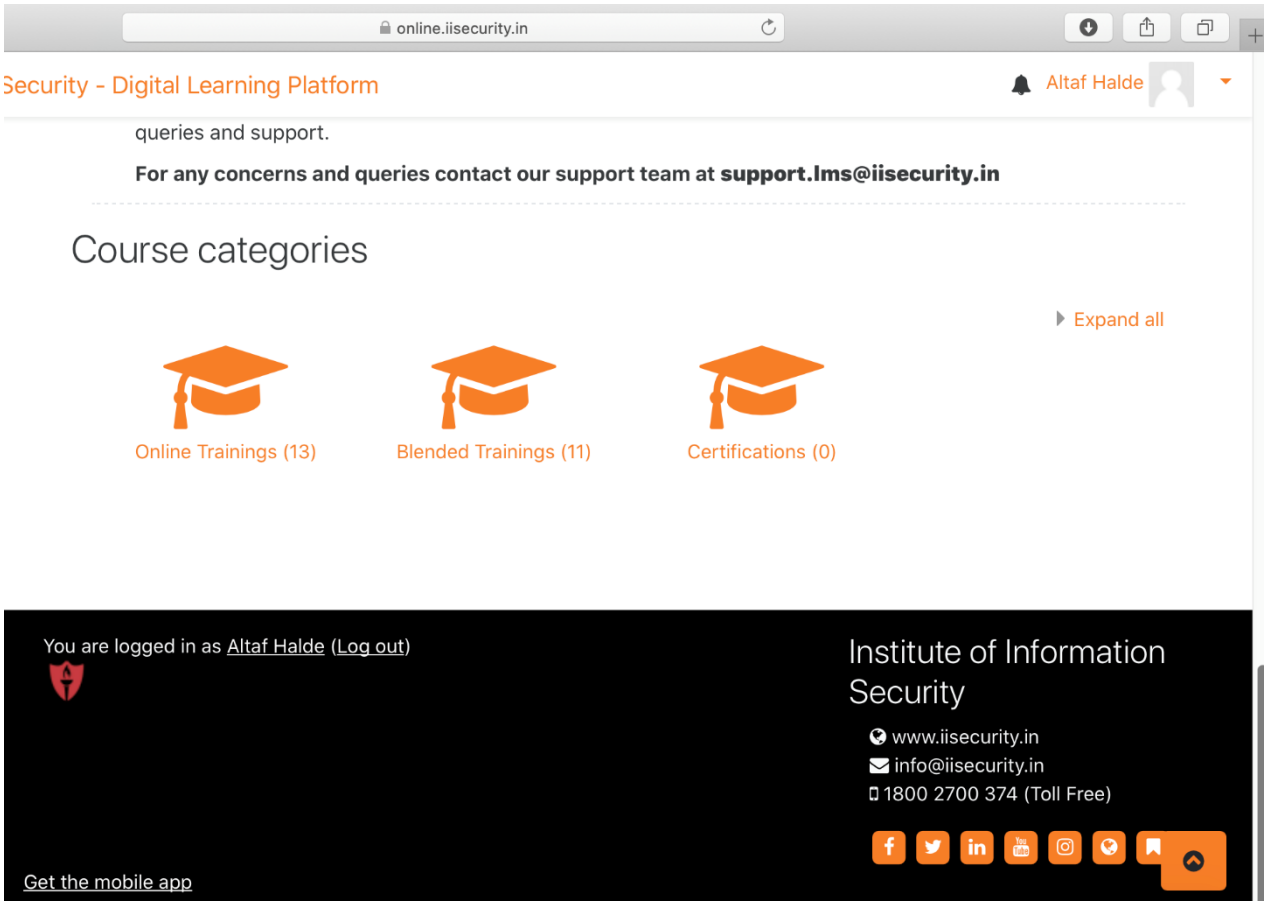


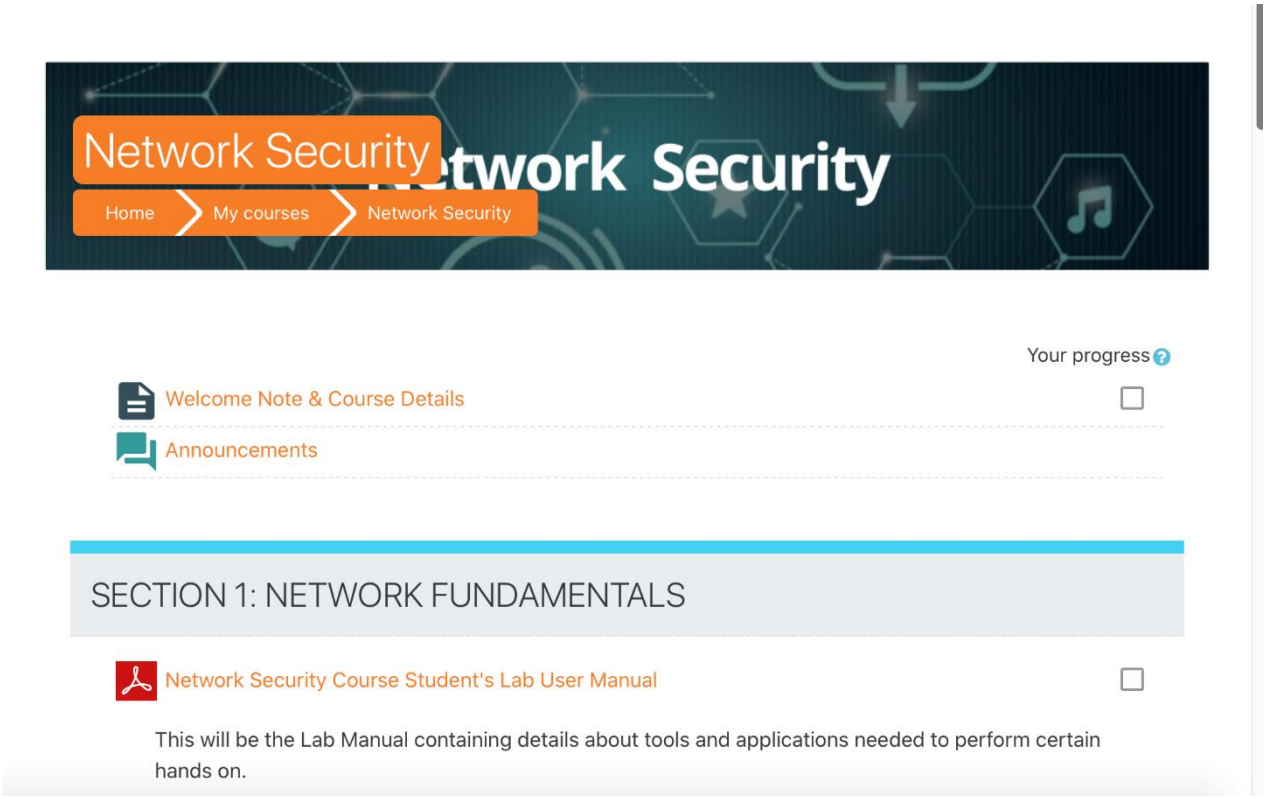

online.iisecurity.in
Institute of Information Security - Digital Learning Platform
Altaf Halde
Home
Dashboard
Calendar
My courses
Network Security
Online - Operating Systems Security
Online - Database Security
Online - Advanced Network Security
Online - Certified Web Application Security Professional (CWASP)
Online - Certified Information Security
Institute of Information Security
IMBIBE • INSPIRE • SHARE
Certified Information Security Consultant (CISC)


online.iisecurity.in
Institute of Information Security - Digital Learning Platform
Altaf Halde
Network Security
Online - Certified Web Application Security Professional (CWASP)
Online - Certified Information Security Consultant (CISC)
Online - Certified Cybersecurity Analyst (CCA)
Online - Mobile Application Security
Online - Certified Professional Hacker + (CPH+)
Online - Certified Cybersecurity Expert (CCE)
More...
Institute of Information Security
IMBIBE • INSPIRE • SHARE
MINIMUM
Certified in Governance, Risk Management & Compliance (CGRC)


online.iisecurity.in
Security - Digital Learning Platform
Altaf Halde
Dashboard
Calendar
Badges
All Courses
Hello ,Welcome to IIS - Digital Learning Platform.
IIS-Digital Learning Platform is designed to enhance your cybersecurity career through well structured training courses in various cybersecurity domains.
Activities
Forums
Resources
Latest announcements
(No announcements have been posted yet.)
IIS Digital Learning Platform Introduction Video


online.iisecurity.in
Security - Digital Learning Platform
Altaf Halde
IIS Digital Learning Platform Introduction Video
This video is about the usage of Digital learning Platform. Kindly watch the video then you can download the IIS Digital Learning Platform Student's User Manual in order to understand the way to work with Digital Learning Platform and rules to be followed while using Digital Learning Platform.
Trainer Profiles
This page provides the Trainer Profiles Details.
IIS-Digital Learning Platform Student's User Manual.
This guide will help you in understanding how to attend courses, submit assignments, attempt quizzes and other information.
Support Forum
This Forum can be used by users in order to communicate with our support team regarding any issues, queries and support.
For any concerns and queries contact our support team at support.lms@iisecurity.in


online.iisecurity.in
Security - Digital Learning Platform
Altaf Halde
queries and support.
For any concerns and queries contact our support team at support.lms@iisecurity.in
Course categories
Expand all
Online Trainings (13)
Blended Trainings (11)
Certifications (0)
You are logged in as Altaf Halde (Log out)
Institute of Information Security
www.iisecurity.in
info@iisecurity.in
1800 2700 374 (Toll Free)
Get the mobile app


Network Security
Home
My courses
Network Security
Your progress
Welcome Note & Course Details
Announcements
SECTION 1: NETWORK FUNDAMENTALS
Network Security Course Student's Lab User Manual
This will be the Lab Manual containing details about tools and applications needed to perform certain hands on.

- 1. Introduction to Network - Theory
- 2. OSI Model - Theory
- 3. TCP/IP Model - Theory
- 4. IPv4 - Theory
- 5. Introduction to Subnetting and Supernetting - Theory
- 6. Routing - Theory
- 7. Router Security and Network Address Translation - Theory
- 8. Switching and Port Security - Theory
- 8.A - Router and Switch Configuration using CPT - Lab
- 8.B - Router and Switch Configuration using CPT - Hands On
- 9. Virtual Local Area Network (VLAN) - Theory
- 10. Virtual Private Network (VPN) - Theory
- 11. Access Control Lists - Theory
- 12. Firewall and IP tables - Theory
- 13. IDS and IPS - Theory
- 14. Packet Capture and Wireshark - Theory
- 14.A - Wireshark - Lab
- 14.B - Understanding TCP IPV4 Headers Using Wireshark - Lab
- 14.C - Understanding TCP IPV4 Headers Using Wireshark - Lab 2
- 14.D - Understanding UDP Header Using Wireshark - Lab
- 14.E - Wireshark - Hands On
- Explain details IPv6 Extension Header - Assignment

  This is the assignment which needs to be completed.
- Make a list of 10 peer to peer websites. - Assignment

  This is the assignment which needs to be completed.
- Section 1 - Network Fundamentals Quiz

  As you have already learnt various concepts related to network fundamentals lets try attempting a quiz in order to find out your progress in this section.

SECTION 2: INTRODUCTION TO NETWORK SECURITY

Restricted Not available unless: The activity **Section 1 - Network Fundamentals Quiz** is marked complete

SECTION 3: NMAP BASICS

Restricted Not available unless: The activity **Section 2 - Introduction to Network Security Quiz** is marked complete

SECTION 4: ENUMERATION

Restricted Not available unless: The activity **Section 3 - Nmap Basics Quiz** is marked complete

SECTION 5: WIRELESS EXPLOITATION

Restricted Not available unless: The activity **Section 4 - Enumeration Quiz** is marked complete

NETWORK SECURITY EXAMINATION

Restricted Not available unless: The activity **Feedback Form** is marked complete

NOTIFICATION

Restricted Not available unless: The activity **NETWORK SECURITY EXAMINATION** is marked complete

|| END OF DOCUMENT ||

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: _____

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[✔] Addendum No. 1	[ ] Addendum No. 6
[✔] Addendum No. 2	[ ] Addendum No. 7
[✔] Addendum No. 3	[ ] Addendum No. 8
[ ] Addendum No. 4	[ ] Addendum No. 9
[ ] Addendum No. 5	[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Network Intelligence, LLC.
Company

Authorized Signature

September 16th 2020
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

Harvard Business Services, Inc.

Address: 16192 Coastal Hwy Lewes, DE 19958 USA

Website: www.delawareinc.com Email: filings@delawareinc.com

Toll Free: (800) 345-2677 Direct: (302) 645-7400 Fax: (302) 645-1280

May 21, 2018

Mr. Kanwal Kumar Mookhey
5th Floor, Lotus Business Park
Mumbai , 400053
India

Dear Mr. Mookhey,

We would like to convey our congratulations to you and Network Intelligence LLC. We hope you enjoy terrific success with your company.

Below is the Employer Identification Number the IRS has generated for your new company:

36-4899565

Please note that if you ever change the name of your company the IRS will need to be notified of this change.

We would like to thank you once again, and wish you the best of luck. You can help us by telling a friend or business associate about our services. We work hard to keep things simple for you and your associates when it's time to incorporate.

Thank you,

Harvard Business Services, Inc.
Business Filings Team

EC-Council

CIRCLE OF EXCELLENCE AWARD

2018

INSTITUTE OF INFORMATION SECURITY SOUTH ASIA

Thank you for your dedication to
Information Security Education

EC-Council

Jay Bavisi, President