Solicitation Number: 34-21

Technical and Price Proposal

Cybersecurity Solutions, Malware, Ransomware Protection, and Other Related Products, and Services

National Cooperative Purchasing Alliance

Due Date: November 18th, 2021 — 2:00 pm CST

Submitted to:

National Cooperative Purchasing Alliance

P.O. Box 701273
Houston, TX 77270

Submitted by:

Global Solutions Group, Inc.

25900 Greenfield Road, Suite 220
Oak Park, MI 48237

Offeror

Global Solutions Group, Inc.
25900 Greenfield Road, Suite 220
Oak Park, MI 48237
www.GlobalSolGroup.com

CAGE 6M9L5
DUNS [redacted]

Socioeconomic Status

Certified EDWOSB
SBA Economically Disadvantaged Woman-Owned Small Business
SBA 8(a) Certified
SBA WOSB Woman Owned Small Business
CERTIFIED NMSDC MBE

Contracting Vehicles

GSA Schedule 36 Contract Holder GS-03F-132DA

GSA IT Schedule 70 Contract Holder GS-35F-171AA

GSA Schedule 736 Contract Holder GS-02F-025GA

GSG has converted each of the above contracts for the MAS consolidation.

Persons authorized to negotiate with the Government and sign the proposal and subsequent award on Offeror's behalf:

Lisa Salvador, Vice President
Direct: (248) 291-5440
Mobile: (313) 333-0188
lisas@globalsolgroup.com

Acknowledgement of Addenda, Questions and Answers, and other Modifications

N/A.

Submit to

National Cooperative Purchasing Alliance

NCPA National Cooperative Purchasing Alliance

P.O. Box 701273
Houston, TX 77270

November 16, 2021

National Cooperative Purchasing Alliance
P.O. Box 701273
Houston, TX 77270

Subject: Global Solutions Group's response to **Solicitation Number 34-21** for **Cybersecurity Solutions, Malware, Ransomware Protection, Other Related Products, and Services**

Dear Sir/Madam:

Global Solutions Group, Inc. (GSG) hereby presents our proposal to provide Cybersecurity Solutions, Malware, Ransomware Protection, Other Related Products, and Services to the National Cooperative Purchasing Alliance (NCPA).

GSG is a multifaceted technology company incorporated in the State of Michigan in 2003. We are headquartered in Oak Park, Michigan. ***We are an SBA 8(a) Certified Small Business, Certified Women Owned Small Business (WOSB), Certified Minority Business Enterprise (MBE), and Economically Disadvantaged Woman — Owned Small Business (EDWOSB).***

We understand that Region 14 Education Service Center (Region 14 ESC) is looking to establish a Master Services Agreement for a wide range of cybersecurity related products and services that will be made available to members of the National Cooperative Purchasing Alliance. This contract will allow agencies to purchase cybersecurity products and services on an "as needed" basis from a competitively awarded contract.

GSG is an ISO/IEC 27001:2013 certified firm. Our cyber team has extensive experience with industry standards and best practices including NIST CSF, FISMA, FedRAMP, PCI–DSS, OWASP, CIS–CSC for Effective Cyber Defense, and others. Our expertise extends to a wide array of IT and cybersecurity technologies such as HPE, Micro Focus, IBM, Splunk, Palo Alto, FireEye, Fortinet, and Cisco, as well as premier cloud technologies such as AWS and Azure.

GSG's Cybersecurity Clients

Our certified cybersecurity and IT specialists are here to provide a comprehensive approach to the NCPA's Cybersecurity Solutions, Malware, Ransomware Protection, Other Related Products, and Services. Our team is experienced in identifying our clients' strengths and vulnerabilities as well as in reviewing policy requirements to ensure compliance. Our mission is characterized by a desire to form

and maintain good client relationships, provide exceptional work performance, and continuously enhance our professional credentials.

GSG is authorized reseller of Ingram Micro for all products.

GSG has a strategic product perspective partnership with Ingram Micro (our partnership is hereafter referred to as 'Team GSG'). Ingram Micro is a global leader in technology and supply chain services. With its vast global infrastructure and focus on cloud, mobility, technology lifecycle, supply chain, and technology solutions, Ingram Micro enables business partners to operate more efficiently and successfully in the markets they serve. Ingram Micro amplifies the value of its position at the intersection of thousands of vendors, reseller, and retailer partners by customizing and delivering highly targeted applications for industry verticals, business to business customers and commercial needs. From provisioning solutions for system integrators working at the heart of the network to offerings through the full lifecycle of mobile devices, SMB to global enterprise software and computing, point of sale to cloud services, professional AV to physical security. Ingram Micro has been providing and sold products and services requested in this requirement for over 20 years to state agencies, local governments, independent school districts, and institutions of higher education. The company supports global operations by way of an extensive sales and distribution network throughout North America, Europe, the Middle East, Africa, Latin America, and the Asia Pacific region.

Team GSG understands that NCPA is seeking Cybersecurity Solutions, Malware, Ransomware Protection, Other Related Products and Services requirements and we need to provide products and services that include, but are not limited to the following points:

- **Identify** — Develop the organizational understanding to manage cybersecurity risk to systems.
- **Protect** — Develop and implement the appropriate safeguards to ensure the continuing delivery of critical infrastructure services.
- **Detect** — Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** — Develop and implement the appropriate activities to respond to detected threats.
- **Recover** — Restore any data, applications, operating systems, configurations, or settings that were corrupted or lost to the threat.

GSG recently awarded a task order to provide IT Security Services and Solutions to [redacted]

GSG is under contract with [redacted] ***to provide Cybersecurity Compliance Assistance Services.***

GSG has provided Network Penetration Testing at the [redacted].

GSG recently completed an IT Security Assessment for the [redacted]

GSG has provided External Network & Web Application Vulnerability Scanning and Penetration Testing to the [redacted].

GSG was recently awarded a multiyear cybersecurity assessment contract by the [redacted]

GSG is currently working on a $10 million BPA for Cybersecurity Assessments and Penetration Testing for the [redacted]

GSG has completed a multiyear contract to provide Federal Information Security Management Act of 2014 (FISMA) Cybersecurity Audit Analysis Services for the [redacted].

Envisioning success for this program requires the highest level of service, ensuring that we operate efficient, agile, high-quality testing and security assessment services that are cost-effective and in compliance with all current regulatory directives and industry standards.

> ***"The GSG Team invested a great deal in training and purchasing the newest and finest tools and licenses available to exceed regulatory requirements. These investments were over and above what was required to perform the work and resulted in a better product which was a benefit to the Government."***
>
> [redacted]

Point of Contact Details

Name: [redacted]
Title: [redacted]
Email: [redacted]roup.com
Telephone: [redacted]

As Vice President of Global Solutions Group, Inc., I am fully authorized to negotiate and bind GSG during the period in which the County is evaluating proposals. You may contact me at any time.

Regards,

Lisa Salvador, Vice President

Table of Contents

Tab 1 – Master Agreement General Terms and Conditions

Signature Form

Signature Form

The undersigned hereby proposes and agrees to furnish goods and/or services in strict compliance with the terms, specifications and conditions at the prices proposed within response unless noted in writing. The undersigned further certifies that he/she is an officer of the company and has authority to negotiate and bind the company named below and has not prepared this bid in collusion with any other Respondent and that the contents of this proposal as to prices, terms or conditions of said bid have not been communicated by the undersigned nor by any employee or agent to any person engaged in this type of business prior to the official opening of this proposal.

Prices are guaranteed: **120 days**

Company name	Global Solutions Group, Inc.
Address	25900 Greenfield Road, Suite 220
City/State/Zip	Oak Park, MI 48237

[redacted]

Tab 2 – NCPA Administration Agreement

Tab 2 – NCPA Administration Agreement

This Administration Agreement is made as of _____, by and between National Cooperative Purchasing Alliance ("NCPA") and Global Solutions Group, Inc. ("Vendor").

Recitals

WHEREAS, Region 14 ESC has entered into a certain Master Agreement dated _____, referenced as Contract Number _____, by and between Region 14 ESC and Vendor, as may be amended from time to time in accordance with the terms thereof (the "Master Agreement"), for the purchase of Cyber-Security Solutions, Malware, Ransomware Protection, Other Related Products and Services ;

WHEREAS, said Master Agreement provides that any state, city, special district, local government, school district, private K-12 school, technical or vocational school, higher education institution, other government agency or nonprofit organization (hereinafter referred to as "public agency" or collectively, "public agencies") may purchase products and services at the prices indicated in the Master Agreement;

WHEREAS, NCPA has the administrative and legal capacity to administer purchases under the Master Agreement to public agencies;

WHEREAS, NCPA serves as the administrative agent for Region 14 ESC in connection with other master agreements offered by NCPA

WHEREAS, Region 14 ESC desires NCPA to proceed with administration of the Master Agreement;

WHEREAS, NCPA and Vendor desire to enter into this Agreement to make available the Master Agreement to public agencies on a national basis;

NOW, THEREFORE, in consideration of the payments to be made hereunder and the mutual covenants contained in this Agreement, NCPA and Vendor hereby agree as follows:

- General Terms and Conditions
  - The Master Agreement, attached hereto as Tab 1 and incorporated herein by reference as though fully set forth herein, and the terms and conditions contained therein shall apply to this Agreement except as expressly changed or modified by this Agreement.
  - NCPA shall be afforded all of the rights, privileges and indemnifications afforded to Region 14 ESC under the Master Agreement, and such rights, privileges and indemnifications shall accrue and apply with equal effect to NCPA under this Agreement including, but not limited to, the Vendor's obligation to provide appropriate insurance and certain indemnifications to Region 14 ESC.
  - Vendor shall perform all duties, responsibilities and obligations required under the Master Agreement in the time and manner specified by the Master Agreement.
  - NCPA shall perform all of its duties, responsibilities, and obligations as administrator of purchases under the Master Agreement as set forth herein, and Vendor acknowledges that NCPA shall act in the capacity of administrator of purchases under the Master Agreement.
  - With respect to any purchases made by Region 14 ESC or any Public Agency pursuant to the Master Agreement, NCPA (a) shall not be construed as a dealer, re-marketer, representative, partner, or agent of any type of Vendor, Region 14 ESC, or such Public

Agency, (b) shall not be obligated, liable or responsible (i) for any orders made by Region 14 ESC, any Public Agency or any employee of Region 14 ESC or Public Agency under the Master Agreement, or (ii) for any payments required to be made with respect to such order, and (c) shall not be obligated, liable or responsible for any failure by the Public Agency to (i) comply with procedures or requirements of applicable law, or (ii) obtain the due authorization and approval necessary to purchase under the Master Agreement. NCPA makes no representations or guaranties with respect to any minimum purchases required to be made by Region 14 ESC, any Public Agency, or any employee of Region 14 ESC or Public Agency under this Agreement or the Master Agreement.

- The Public Agency participating in the NCPA contract and Vendor may enter into a separate supplemental agreement to further define the level of service requirements over and above the minimum defined in this contract i.e. invoice requirements, ordering requirements, specialized delivery, etc. Any supplemental agreement developed as a result of this contract is exclusively between the Public Agency and Vendor. NCPA, its agents, members and employees shall not be made party to any claim for breach of such agreement.

- Term of Agreement
  - This Agreement shall be in effect so long as the Master Agreement remains in effect, provided, however, that the obligation to pay all amounts owed by Vendor to NCPA through the termination of this Agreement and all indemnifications afforded by Vendor to NCPA shall survive the term of this Agreement.

- Fees and Reporting
  - The awarded vendor shall electronically provide NCPA with a detailed quarterly report showing the dollar volume of all sales under the contract for the previous quarter. Reports are due on the fifteenth (15th) day after the close of the previous quarter. It is the responsibility of the awarded vendor to collect and compile all sales under the contract from participating members and submit one (1) report. The report shall include at least the following information as listed in the example below:

Entity Name	Zip Code	State	PO or Job #	Sale Amount

Total _____

  - Each quarter NCPA will invoice the vendor based on the total of sale amount(s) reported. From the invoice the vendor shall pay to NCPA an administrative fee based upon the tiered fee schedule below. Vendor's annual sales shall be measured on a calendar year basis. Deadline for term of payment will be included in the invoice NCPA provides.

Annual Sales Through Contract	Administrative Fee
0 - $30,000,000	2%
$30,000,001 - $50,000,000	1.5%
$50,000,001+	1%

- Supplier shall maintain an accounting of all purchases made by Public Agencies under the Master Agreement. NCPA and Region 14 ESC reserve the right to audit the accounting for a period of four (4) years from the date NCPA receives the accounting. In the event of such an audit, the requested materials shall be provided at the location designated by Region 14 ESC or NCPA. In the event such audit reveals an under reporting of Contract Sales and a resulting underpayment of administrative fees, Vendor shall promptly pay NCPA the amount of such underpayment, together with interest on such amount and shall be obligated to reimburse NCPA's costs and expenses for such audit.

- General Provisions
  - This Agreement supersedes any and all other agreements, either oral or in writing, between the parties hereto with respect to the subject matter hereof, and no other agreement, statement, or promise relating to the subject matter of this Agreement which is not contained herein shall be valid or binding.
  - Awarded vendor agrees to allow NCPA to use their name and logo within website, marketing materials and advertisement. Any use of NCPA name and logo or any form of publicity regarding this contract by awarded vendor must have prior approval from NCPA.
  - If any action at law or in equity is brought to enforce or interpret the provisions of this Agreement or to recover any administrative fee and accrued interest, the prevailing party shall be entitled to reasonable attorney's fees and costs in addition to any other relief to which such party may be entitled.
  - Neither this Agreement nor any rights or obligations hereunder shall be assignable by Vendor without prior written consent of NCPA, provided, however, that the Vendor may, without such written consent, assign this Agreement and its rights and delegate its obligations hereunder in connection with the transfer or sale of all or substantially all of its assets or business related to this Agreement, or in the event of its merger, consolidation, change in control or similar transaction. Any permitted assignee shall assume all assigned obligations of its assignor under this Agreement.
  - This Agreement and NCPA's rights and obligations hereunder may be assigned at NCPA's sole discretion, to an existing or newly established legal entity that has the authority and capacity to perform NCPA's obligations hereunder
  - All written communications given hereunder shall be delivered to the addresses as set forth below.

National Cooperative Purchasing Alliance:		**Vendor:**	Global Solutions Group, Inc.
Name:		Name:	[redacted]
Title:		Title:	
Address:		Address:	25900 Greenfield Road, Suite 220 Oak Park, MI 48237
Signature:		Signature:	[redacted]
Date:		Date:	November 16, 2021

Tab 3 – Vendor Questionnaire

Tab 3 – Vendor Questionnaire

Please provide responses to the following questions that address your company's operations, organization, structure, and processes for providing products and services.

- States Covered
  - Bidder must indicate any and all states where products and services can be offered.
  - Please indicate the price co-efficient for each state if it varies.

☒ **50 States & District of Columbia** (Selecting this box is equal to checking all boxes below)

☐ Alabama	☐ Maryland	☐ South Carolina
☐ Alaska	☐ Massachusetts	☐ South Dakota
☐ Arizona	☐ Michigan	☐ Tennessee
☐ Arkansas	☐ Minnesota	☐ Texas
☐ California	☐ Mississippi	☐ Utah
☐ Colorado	☐ Missouri	☐ Vermont
☐ Connecticut	☐ Montana	☐ Virginia
☐ Delaware	☐ Nebraska	☐ Washington
☐ District of Columbia	☐ Nevada	☐ West Virginia
☐ Florida	☐ New Hampshire	☐ Wisconsin
☐ Georgia	☐ New Jersey	☐ Wyoming
☐ Hawaii	☐ New Mexico	
☐ Idaho	☐ New York	
☐ Illinois	☐ North Carolina	
☐ Indiana	☐ North Dakota	
☐ Iowa	☐ Ohio	
☐ Kansas	☐ Oklahoma	
☐ Kentucky	☐ Oregon	
☐ Louisiana	☐ Pennsylvania	
☐ Maine	☐ Rhode Island	

☒ **All US Territories and Outlying Areas** (Selecting this box is equal to checking all boxes below)

- ☐ American Somoa
- ☐ Federated States of Micronesia
- ☐ Guam
- ☐ Midway Islands
- ☐ Northern Marina Islands
- ☐ Puerto Rico
- ☐ U.S. Virgin Islands

- Minority and Women Business Enterprise (MWBE) and (HUB) Participation
  - It is the policy of some entities participating in NCPA to involve minority and women business enterprises (MWBE) and historically underutilized businesses (HUB) in the purchase of goods and services. Respondents shall indicate below whether or not they are an M/WBE or HUB certified.
    - Minority / Women Business Enterprise
      - Respondent Certifies that this firm is a M/WBE ☒
    - Historically Underutilized Business
      - Respondent Certifies that this firm is a HUB ☐
- Residency
  - Responding Company's principal place of business is in the city of Oak Park, State of Michigan
- Felony Conviction Notice
  - Please Check Applicable Box:
    - ☐ A publically held corporation; therefore, this reporting requirement is not applicable.
    - ☒ Is not owned or operated by anyone who has been convicted of a felony.
    - ☐ Is owned or operated by the following individual(s) who has/have been convicted of a felony
  - If the 3rd box is checked, a detailed explanation of the names and convictions must be attached.
- Distribution Channel
  - Which best describes your company's position in the distribution channel:
    - ☐ Manufacturer Direct
    - ☒ Authorized Distributor
    - ☒ Value-added reseller
    - ☐ Certified education/government reseller
    - ☐ Manufacturer marketing through reseller
    - ☐ Other: _____
- Processing Information
  - Provide company contact information for the following:
    - Sales Reports / Accounts Payable

      Contact Person: Sahil Shah
      Title: Controller
      Company: Global Solutions Group, Inc.
      Address: 25900 Greenfield Road, Suite 220
      City: Oak Park State: Michigan Zip: 48237
      Phone: 248.850.8763 Email: sahils@globalsolgroup.com

- Purchase Orders

  Contact Person: Lisa Salvador
  Title: Vice President
  Company: Global Solutions Group, Inc.
  Address: 25900 Greenfield Rd., Suite 220
  City: Oak Park State: MI Zip: 48237
  Phone: 248.291.5440 Email: lisas@globalsolgroup.com

[redacted]

- Pricing Information
  - In addition to the current typical unit pricing furnished herein, the Vendor agrees to offer all future product introductions at prices that are proportionate to Contract Pricing.
    - If answer is no, attach a statement detailing how pricing for NCPA participants would be calculated for future product introductions.

      [X] Yes [ ] No
  - Pricing submitted includes the required NCPA administrative fee. The NCPA fee is calculated based on the invoice price to the customer.

    [X] Yes [ ] No
  - Vendor will provide additional discounts for purchase of a guaranteed quantity.

    [X] Yes [ ] No

- Cooperatives
  - List any other cooperative or state contracts currently held or in the process of securing.

Cooperative/State Agency	Discount Offered	Expires	Annual Sales Volume
[redacted]	[redacted]	[redacted]	[redacted]

Tab 4 – Vendor Profile

Company's official registered name.

Global Solutions Group, Inc.

Brief history of your company, including the year it was established.

GSG was founded in 2003 to provide IT support services to government agencies as well as private sector clients. We are incorporated pursuant to the laws of the State of Michigan, and our offices are in Oak Park, Michigan.

As our IT consulting business grew, we recognized that several of our clients were not satisfied with their existing information security services, so we started placing IT Security professionals with those clients. That experience has allowed us to expand our IT services to include cybersecurity consulting. We have since added cybersecurity audits, assessments, and penetration testing as key facets of our business. Our cybersecurity expertise has led to major multiyear contracts with the AbilityOne Commission as well as a multiyear, multimillion-dollar contract to provide operational assessment and penetration testing to all offices and agencies under the purview of the USDA nationwide.

We have several strategic partnerships which provide our teams with additional resources, enabling them to provide additional value to our clients:

As a small business, GSG is agile in adjusting our approach to meet the specific needs of each client — whether it is a commercial operation, a state agency, or an entire Cabinet-level department with locations across the nation.

- For our $9.8 million BPA contract with the [redacted] we are providing operational risk assessment, penetration testing, web security assessment with high-value applications, and Red Team Assessment for the [redacted], which processes payroll for over 600,000 federal government employees. Our team is also conducting FISMA/FedRAMP-based vulnerability assessments and penetration testing.
- GSG is recently awarded a contract of $1.9 million to provide Cybersecurity Assessment Service Support for the [redacted].
- GSG provided Network Penetration Testing to the [redacted] This project consisted of external and internal penetration testing of JAA's network with the goal of

obtaining access to protected data in four categories: Access Control, Law Enforcement & Criminal Justice Information System Compliance, PCI Compliance, and General Security.

- GSG recently completed a contract for the [redacted] Our team performed a full IT security assessment, including multiple assessments of the internal and external networks, review of network device configurations, application and wireless penetration testing, and social engineering efforts.
- We recently completed a major multiyear contract with the [redacted] to provide Federal Information Security Management Act of 2014 (FISMA) Analysis Services.
- GSG has performed multiple task orders under contract to the [redacted] for cybersecurity support:

[redacted]

Malware Recovery Services

GSG conducted a forensic investigation to determine what data had been exposed, and re-imaged infected workstations. We also ensured that all workstations and servers were patched, that the antivirus was operating correctly, and that it was updated to the latest versions of the signature files and scan engine.

[redacted]

File Permissions Investigation

GSG conducted a forensic investigation of unauthorized high-level access to identify a user who had changed file permissions, allowing access to restricted files. We reviewed all relevant logs to identify a suspect user ID, along with a report detailing the evidence that the identified ID had been used to alter authorizations in a manner not in compliance with Department policies or state and federal regulations.

[redacted]

Application Security Assessment

We conducted external scans using a suite of tools that assess the EpiTrax application from the perspective of an outsider, along with manual verification of vulnerabilities and exploitation of identified application/host vulnerabilities to gain system level access, obtain custom data, or deny service to the application.

[redacted]

Citrix NetScaler Managed Services

GSG provided updates and upgrades to all managed Citrix NetScaler NMAS, SDX, and VPX appliances. These services included project management, status reporting, customer communication, upgrades, and patches.

GSG Provides:

- Cybersecurity Assessments and Penetration Testing services to over **21** sub-agencies of more than **45,000** [redacted] end users located in more than **3,400** field offices across the country
- Cybersecurity assessment services to **15** Data Centers, **105,000** workstations, **15,000** servers and **120,000** Endpoints.
- Scanning of **200,000+** IPs for penetration testing
- Examination and evaluation of the agency's operational security policies, procedures, and systems.
- Identification of strengths, vulnerabilities, and agency security posture
- Identification and evaluation of attacker tools and methods.

[redacted]

Information Security Officer Services

A GSG team member provides security program management for all agencies across the [redacted] We assist all agencies in performing security self-assessments and incident management, developing DR/COOP and information risk management plans, and more.

Our team has extensive experience with the NIST Cybersecurity Framework, Federal Risk and Authorization Management Program (FedRAMP), Payment Card Industry Data Security Standard (PCI–DSS), Open Web Application Security Project (OWASP), Center for Internet Security Critical Security Controls for Effective Cyber Defense, and other standards and practices.

Types of Services Performed

- IT Governance, Compliance & Strategy
- Application/Web Application Security
- Asset Management Design & Implementation
- Database Design & Administration
- Systems Administration
- Systems Engineering/Architecting
- Data/Business Analysis
- Regulatory Compliance
- Log Management
- Penetration Testing
- Security Compliance & Risk Assessment
- NIST, FISMA, PCI DSS, HIPAA, CJIS, ISO, GDPR
- Family Educational Rights and Privacy Act (FERPA)
- Authorization to Operate (ATO)/Authorization to Connect (ATC)
- Interconnection Security Agreement (ISA)
- Vulnerability Assessment Web and Mobile Application Testing
- 24/7/365 Security Operations Center (SOC)
- Security Information and Event Management (SIEM)
- Assessment and Authorization (A&A)
- Risk Management Framework (RMF)
- Incident Response & Management Support
- Training and Awareness
- Cybersecurity Infrastructure
- Privacy Support Planning
- Intrusion Testing
- Physical & Electronics Security
- Assessment, Integration, Automation
- Identity and Access Management
- Embedded/IoT Services and Systems Hardening

Ingram Micro Overview

Ingram Micro is a global leader in technology and supply chain services. With its vast global infrastructure and focus on cloud, mobility, technology lifecycle, supply chain, and technology solutions, Ingram Micro enables business partners to operate more efficiently and successfully in the markets they serve. Ingram Micro amplifies the value of its position at the intersection of thousands of vendors, reseller, and retailer partners by customizing and delivering highly targeted applications for industry verticals, business to business customers and commercial needs. From provisioning solutions for system integrators working at the heart of the network to offerings through the full lifecycle of mobile devices, SMB to global enterprise software and computing, point of sale to cloud services, professional AV to physical security. Ingram Micro has been providing and sold products and services requested in this requirement for over 20 years to state agencies, local governments, independent school districts, and institutions of higher education. The company supports global operations by way of an extensive sales and distribution network throughout North America, Europe, the Middle East, Africa, Latin America, and the Asia Pacific region.

- Local sales offices and/or representatives in 64 countries
- 189 logistics centers and service centers worldwide

- Representing over 2,000 suppliers including Acer, Apple, Cisco, Citrix, HP, IBM, Lenovo, Microsoft, Samsung, Symantec, VMware, and others
- Serving more than 250,000 customers in approximately 160 countries
- Creating growth opportunities within the hard-to-reach SMB market as more businesses use technology to add scale, enhance services and improve productivity
- Providing support from 35,000+ associates worldwide
- The only global broad-based IT distributor with a significant Asia Pacific presence

GSG's Dun & Bradstreet (D&B) number.

078343325

Company's organizational chart of those individuals that would be involved in the contract.

Our organizational structure — based on arranging clear-cut lines of communication, responsibility, and relationships in a straightforward manner — facilitates formal and informal communications between our Contract Manager, Customer Success Manager, and your stakeholders. Regular customer communication (both scheduled and spontaneous) is a critical element in our management approach. We believe that establishing an atmosphere of cooperation, coupled with a clear communication structure, is crucial to resolve or prevent potential unanticipated challenges. At GSG, we strive for transparency in all our client interactions.

GSG's technology solutions are designed to provide the greatest benefit at the lowest cost, with the least possible amount of disruption to our clients' day-to-day activities. We work with our clients to clarify project and program requirements, develop schedules, and ensure performance via predetermined goals and objectives (schedule milestones).

We have a diversely qualified team in place to ensure that exceptional financial, administrative, contractual, and general project performance is provided throughout the duration of the contract. Our personnel will be available to support the Contract Manager and Customer Success Manager as necessary, ensuring correct workflow and mission clarity on each project.

Following is a proposed overall organizational chart that details the primary personnel slated to serve as the main points of contact for NCPA:

Corporate Office Location

Oak Park, Michigan.

List the number of sales and services offices for states being bid in solicitation.

Local sales offices and/or representatives in 64 countries.

Offices: Michigan, California, Maryland

List the names of key contacts at each with title, address, phone, and e-mail address.

[redacted]

Define your standard terms of payment.

Net 30 days.

Who is your competition in the marketplace?

GSG has extensive experience in providing cybersecurity products and services to a broad variety of private and public sector clients. Our capabilities in cybersecurity have been recognized by the award of a multiyear contract to provide Operational Security Assessment, Penetration Testing, and Web Security Assessment services to over 18 component agencies of the USDA at locations across the country, as well as other co-located agencies. With over 18 years of experience providing a full spectrum of IT support for our clients, we have built the capacity and pool of talent needed to expertly and effectively provide any level of cybersecurity support required.

GSG offers 18 years of lessons learned from providing directly relevant work performing on large-scale federal government contracts, as well as on projects for a variety of commercial and non-commercial clients. Through our team's experience in IT services, including our involvement in government, public services, account administration, and data management, we ensure the reduction of risk and the provision of timely, cost-effective services to the satisfaction of all stakeholders.

We have many competitors in the market, including:

- Raytheon Intelligence and Space
- Novacoast
- BitLyft Cybersecurity
- Dewpoint
- Escape Velocity Holding, Inc.
- AT&T / Nordicom
- Sequris Group, LLC / CyberforceQ
- Presidio Networked Solutions

Provide Annual Sales for last 3 years broken out into the following categories:

- **Cities / Counties**

[redacted]

[redacted]

- **K-12**

[redacted]

- **Higher Education**

[redacted]

- **Other government agencies or nonprofit organizations**

[redacted]

What differentiates your company from competitors?

The following table outlines four major parameters which differentiate GSG from our competitors:

Parameters	GSG's Cybersecurity Services	Benefits to NCPA
Highest Quality	• With an approach tailored to meet NCPA's requirements, our team utilizes industry best practices, bleeding-edge technology, and first-rate research to understand, anticipate, and protect against even the most advanced intrusion attempts.	• An IT ecosystem that is hardened against attacks, ensuring continuity of uninterrupted services and security of data that meets all cybersecurity standards.
Personnel Qualifications	• Our key personnel are highly qualified, experienced, and certified. • Certifications include but are not limited to Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), CompTIA Security+, Certified Information Systems Security Professional (CISSP), and SANS GIAC Security Essentials. • We hire certified cybersecurity professionals with high levels of specialized experience and familiarity with cybersecurity risk management processes such as International Organization for Standardization (ISO) 31000:2009, ISO/IEC 27005:2011, National Institute of Standards and Technology (NIST) Special Publication 800-39, and the Electricity	• Experienced professionals are ready to start on from Day 1 from award of this contract. • With high levels of experience in their field, our team ensures timely and efficient project execution. • NCPA can be secure in the knowledge that the most current threat vectors and mitigation strategies have been considered.

Parameters	GSG's Cybersecurity Services	Benefits to NCPA
	Subsector Cybersecurity Risk Management Process (RMP) guidelines.	
Proven Performance	◆ We recently completed Network Penetration and Vulnerability Testing for the [redacted]. ◆ Currently, GSG is working on a multiyear $10 million BPA for Cybersecurity Assessments and Penetration Testing for the [redacted] ◆ We recently completed a multi-year contract to provide Federal Information Security Management Act of 2014 (FISMA) Analysis Services for the [redacted].	◆ A contractor capable of managing and meeting the demands for required cybersecurity services. ◆ Proven capability with long term, complex security assessments.
Capability/ Experience	◆ Personnel with an average of 15 years of experience in IT security support. ◆ Our key personnel have performed hundreds of web application assessments and network penetration tests. ◆ For the [redacted] our key personnel implemented U.S. Government Configuration Baseline standards enterprise-wide (about 2,000 endpoints and servers) with continuous monitoring.	◆ Strong knowledge base of the industry due to work on multiple federal, state, and local projects. ◆ Improved and more reliable measures of confidence in cybersecurity requirements. ◆ Oversight of contract performance and quality assurance using industry standard review techniques and implemented by highly trained and experienced cybersecurity professionals.

Describe how your company will market this contract if awarded.

GSG will create special marketing efforts and distribution materials designed to enhance awareness of our Cybersecurity Products and Services available throughout Region 14 Education Services Center (ESC) and all NCPA participating entities via this contract. Our team will gain marketing insights and leads through participation at government conferences and trade shows attended by government agencies and purchasing officers. We also have an active social media program, and we target public and private sector organizations through social media-based campaigns. Our team monitors multiple public bid platforms, and we leverage our experience and reputation to create winning proposal responses for all levels of government.

GSG reviews a 10-point sales and marketing strategy for each contract to boost profits and gain ground on competitors. We start by breaking down the process into discrete, manageable elements and generate a checklist that can be reviewed to prioritize areas needing improvement and serve as the groundwork for an effective marketing strategy.

1) Markets: We research current and future markets to learn why customers buy from us and what we can add to our offerings to attract more customers. GSG identifies ways to sell more to your most profitable customers, and highlights easily missed opportunities in bulk, institutional, industrial, or

corporate markets beyond normal retail. This data can help us to determine if new features or services will attract new customers or if people will pay more for them.

To collect information, we study what competitors are doing and collect information about other customers. We use surveys to gather information and can establish customer loyalty programs that require participants to register by providing some basic information about themselves. These details can help us figure out which demographics we are attracting — or failing to attract.

2) Competition: Every organization can benefit by knowing who their competitors are and what they are up to. What is the overall market trend, and how are you holding up in terms of market share and profit position? How do you rank against competitors? What substitutes are there to your products, and how much of a threat are they? We use competitive intelligence to maintain and enhance your business's market share. This involves researching what competitors offer, their price points, and what their marketing strategies say about the demographics they are targeting.

3) Distribution: We identify ways to get products or services to new outlets profitably. This could involve increasing web sales, expanding delivery options, contracting with additional retail outlets to carry products, finding mutually beneficial ways to collaborate with other businesses, and more.

4) Supply Chain: Our partner for this engagement, Ingram Micro, is a leading global supplier, and we will take advantage of their supply chain as well as our own to ensure the timely and accurate delivery of goods and services under this contract.

5) Positioning: It is important to know where we fit in the market, and knowing your competition is a big part of this.

6) Promotion: We maximize our chances of reaching potential customers by meeting them where they are. When trying to reach an audience through social media, for example, it's good to know which demographic uses which platforms.

7) Pricing: We constantly review our pricing strategy to be sure it makes sense for everything we offer. Consumer demand, product availability, and other external factors all play a role in our pricing structure.

8) Customer Service: The first step to providing good customer service is understanding the kind of service our customers want. We encourage customer feedback through our open lines of communication, and we are always receptive to client requirements and comments. This contract will have a dedicated Customer Success Manager to ensure that NCPA is satisfied with our services.

9) Financing: GSG reviews our capital structure regularly to make sure we are handling assets and liabilities in the most cost-effective way.

10) Consistent Strategies: Customer loyalty and increasing sales to existing customers is a major goal for GSG. Our focus is on giving our customers superior service that consistently exceeds expectations. Our strategy for doing so focuses on having clear and consistent lines of communication to ensure everything is proceeding according to schedule and budget. Our team always looks for ways to increase value to the customer without increasing the cost.

Sales Strategy

GSG's 10 keys to develop a successful sales strategy:

Order Processing

GSG's order processing involves the following steps:

Order processing requires coordination between different areas — sales, customer care, suppliers, bookkeeping, and managers — to ensure that all orders are processed accurately, in a timely manner, and in compliance with order processing guidelines.

- Ensure all relevant order processing paperwork is submitted in accordance with order guidelines
- Ensure appropriate approvals are in place before processing an order
- Double check all order requirements and fulfillment objectives
- Work closely with the marketing and proposal teams to provide insight on orders and help prioritize schedules
- Work with relevant personnel on non-compliant orders and provide direction and clarity on steps to resolve order issues
- Develop a strong understanding of historical and new orders as well as customer and partner base
- Ensure orders comply with our licensing mechanism(s) and approval processes
- Document order management processes and update documents as processes evolve
- Monitor sales order database as needed

Customer Support

Team GSG believes that the key to good customer support service is building good relationships with our customers. To that end, we have assigned Tom Seagrist, Senior Customer Success Manager, as part of our team for this contract.

Team GSG ensures that we provide the best customer service by:

- Knowing what our customers consider to be good customer service
- Taking the time to find out customers' expectations
- Following up on both positive and negative feedback
- Ensuring that we consider customer service in all aspects of your business
- Continuously looking for ways to improve the level of customer service we deliver

Describe how you intend to introduce NCPA to your company.

GSG will provide marketing materials, logos, and catalogs as required for posting in the vendor section of the NCPA website under the appropriate categories. We will also monitor the solicitations posted on the website.

Describe your firm's capabilities and functionality of your on-line catalog / ordering website.

For all cybersecurity related services rather than products, a detailed, custom quote is required. For those inquiries, contact Lisa Salvador, Vice President of Global Solutions Group, at [redacted] with detailed requirements.

For products offered, Team GSG supports your orders with this process:

- Use carts to build and create orders.
- Once you check out with a cart, that cart becomes an order.
- Track order status and fulfillment with the Help Center features cited in this section.

- Order details may contain serial numbers, shipping method, direct ship information, and more.

Use these easy steps to view and manage orders and invoices:

- Order List
- Order Details
- Order Details (New)
- Invoice Gateway

Order List

Create a new order when complete the checkout process.

The GSG website supports multiple features for tracking and managing orders:

- Order list
- Order history
- Sorting
- Filtering
- Status information
- Tracking order

This page provides instructions for navigating to and managing orders:

- View & Search Orders
- Frequently Asked Questions

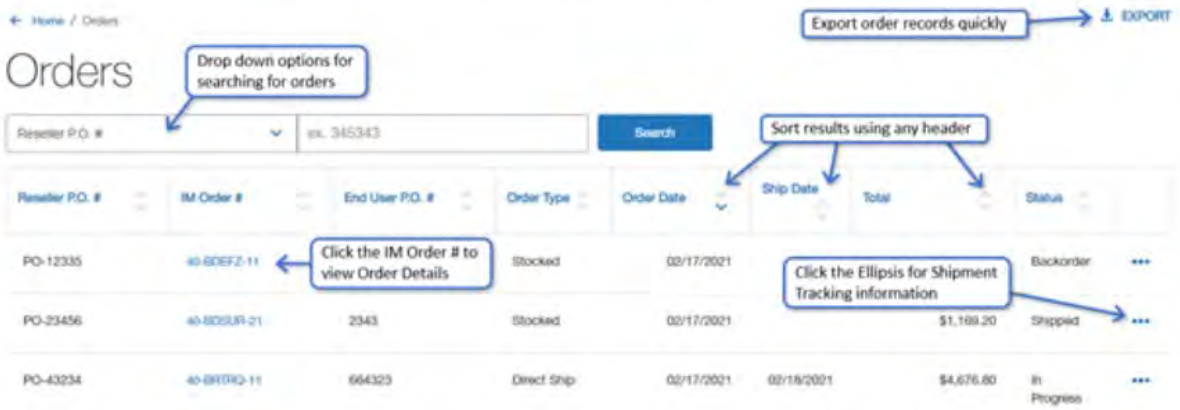
View & Search Orders

Use these steps to view and search orders.

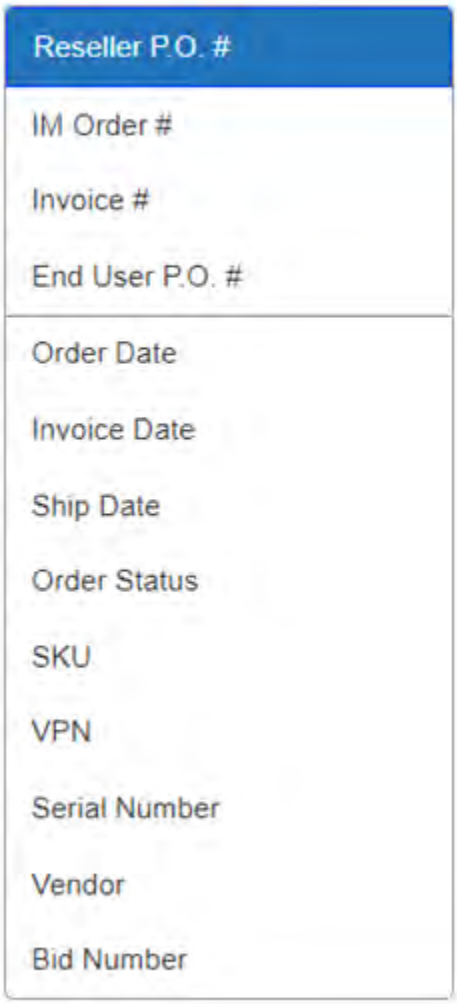
1. Go to the **Orders** page. You have 2 options:
   - Click **Orders**

   - Click My Account icon > **Orders**.

2. On the **Orders** page, you have several options to search, sort, and view additional order details:

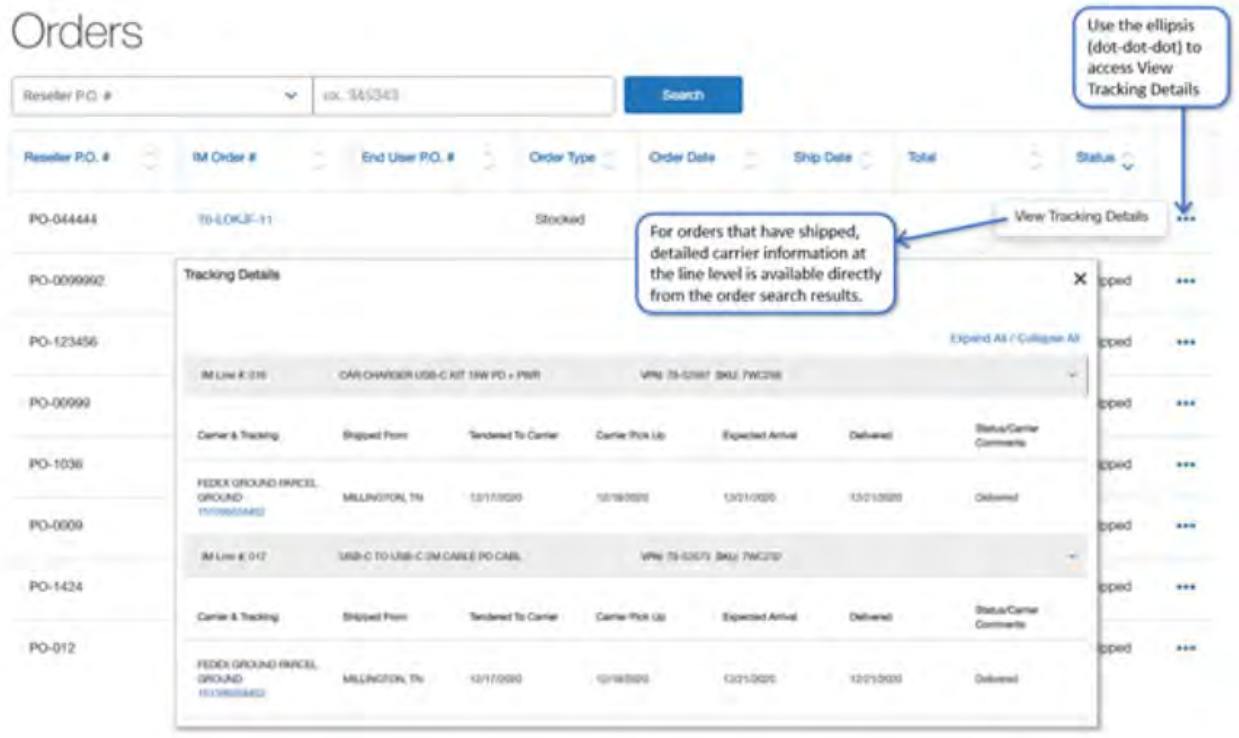


- Search for orders.
- Select a search type then provide the search string.
- Click **Search**.



- Sort orders by any column.

3. From Order Search results for **Shipped** orders, click on three dots (…) and View Tracking Detail.
   - It includes accurate Carrier tracking information at the line level, similar to Tracking Details tab in Order Details
   - Includes carrier, tracking #, ship from, tendered to carrier, pickup, ETA, delivered, status



Frequently Asked Questions

Where can I find information about lost shipments, returns, invoice discrepancies, and similar queries?

Start by using the resources in Services for more information or contact Ingram Micro for immediate assistance.

What should I do if I do not receive any email order confirmations?

- You can configure email notifications by clicking the **My Account** icon > **My Account** > **Notification Preferences**.
- You must enter the email address and select the type of notification to receive.

How can I manage my current orders?

You can access your orders directly from your dashboard.

1. Go to the **Orders** page. You have 2 options:
   - Click **Orders**.
   - Click the **My Account** icon > **Orders**.
2. On the **Orders** page, search or browse for the order to review.
3. On the **Order Details** page, review information specific to each order.

Refer to Orders for additional how-to information.

How do I order a product?

Once you have a registered account with Ingram Micro, search and browse products and vendors to view complete information. From **Product Details**, add items to your cart by entering a quantity and clicking **Add**.

Refer to Search & Browse and Orders for more information.

Can I place an order on hold?

Yes. To place an order on hold:

1. Go to the **Cart** > **Checkout** page. Click **Place Order on Hold** on the **Checkout** page.
   - On-hold orders will be displayed with an On Hold status in the order summary page.
   - You will be informed of the date when the hold will expire.
2. You must submit, modify, or cancel the order before that date or it will be automatically voided.

Can I reorder a past order?

Yes, to submit a past order as a new order:

1. Go to the **Orders** page. You have 2 options:
   - Click **Orders**.
   - Click the **My Account** icon > **Orders**.
2. Display the **Order Details** page for the order to create into a new order.
3. Click **Add Contents for Re-order** button on the **Order Details** page.
4. From the drop-down menu, select an existing cart or create a new cart.

Back to top

Order Details

Any order provides details for a variety of information:

- PO numbers
- Addresses
- Status
- Use an existing order to create a new cart
- more

You can view changes in order status and set up notifications.

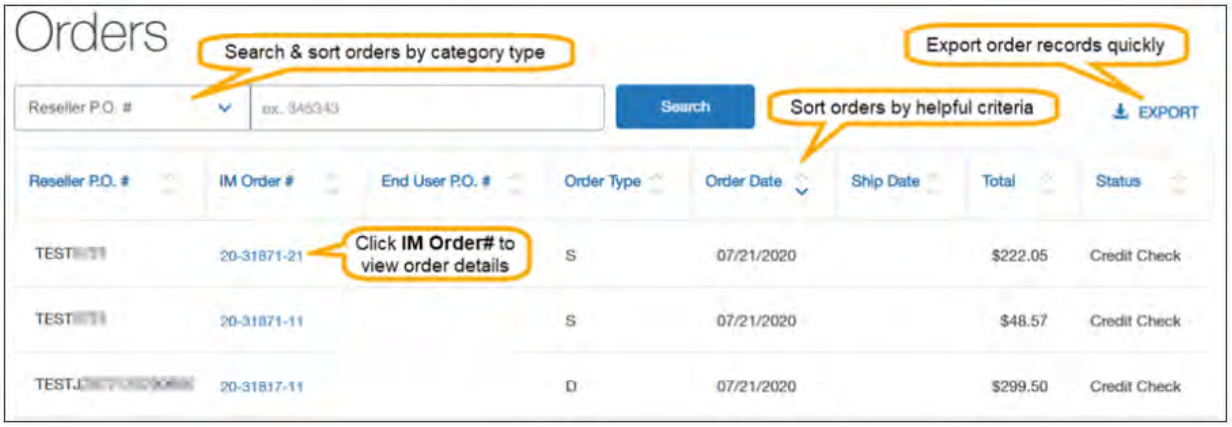
View Order Details

Use these steps to view order details:

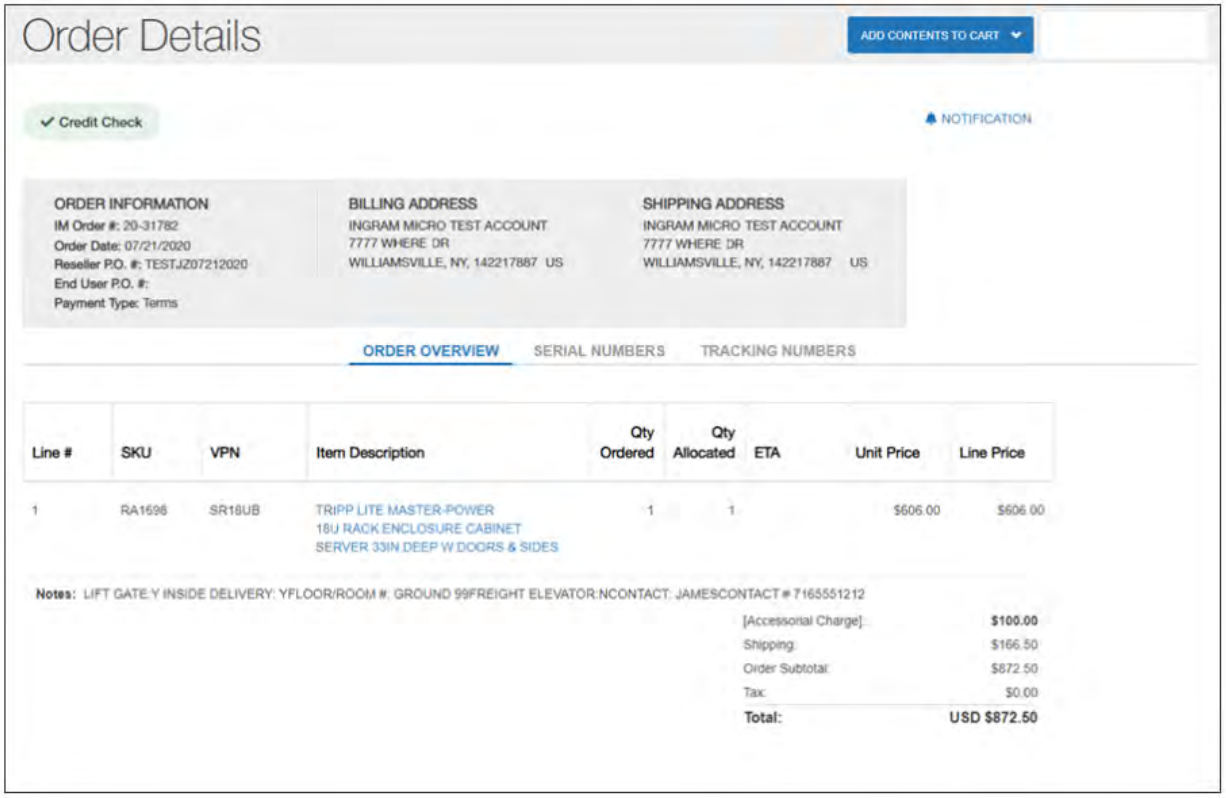
1. Go to the **Orders** page. You have 2 options:
   - Click **Orders**

   - Click **My Account** icon > **Orders**.

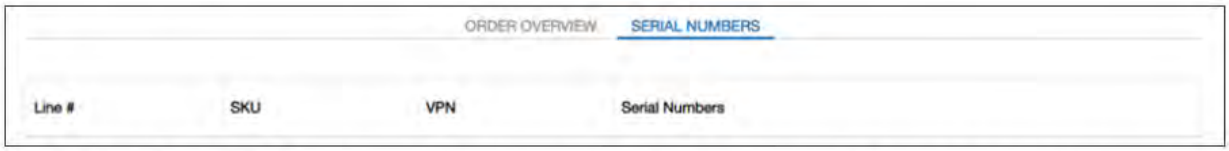
     The **Order List** screen shows the order history.



2. On the **Order List** screen, click any **IM Order#** to show **Order Details.**

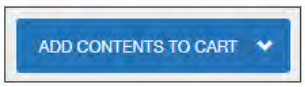


- **ORDER OVERVIEW**: Lists each line item in the order with available product information.
- **SERIAL NUMBERS**: Contains the SKU, VPN and serial numbers for each line item in the order, as available.

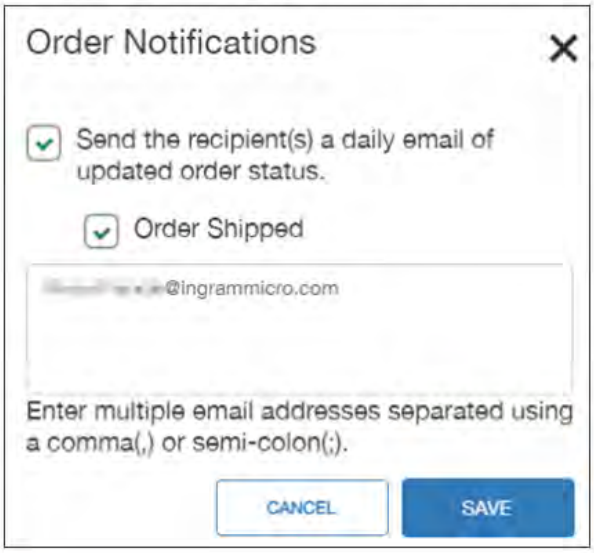


- **TRACKING NUMBERS**: Provides available shipping information by tracking number, when this is available.

- **ADD CONTENTS TO CART**: Use this feature to copy all items in this order into the active cart. This is a convenient way to manage carts and orders if you often order the same products.



- **SUBMIT RETURNS OR CLAIMS:** Use this feature (when available) to navigate to the Returns Management page. Refer to Returns and RMA.
- **NOTIFICATIONS:** You can set up or adjust notifications for any order:
  - Click **NOTIFICATION** from the **Order Details** page.
  - On the **Order Notifications** page, edit information and click **SAVE**.



Back to top

Order Details

Any order provides details for a variety of information:

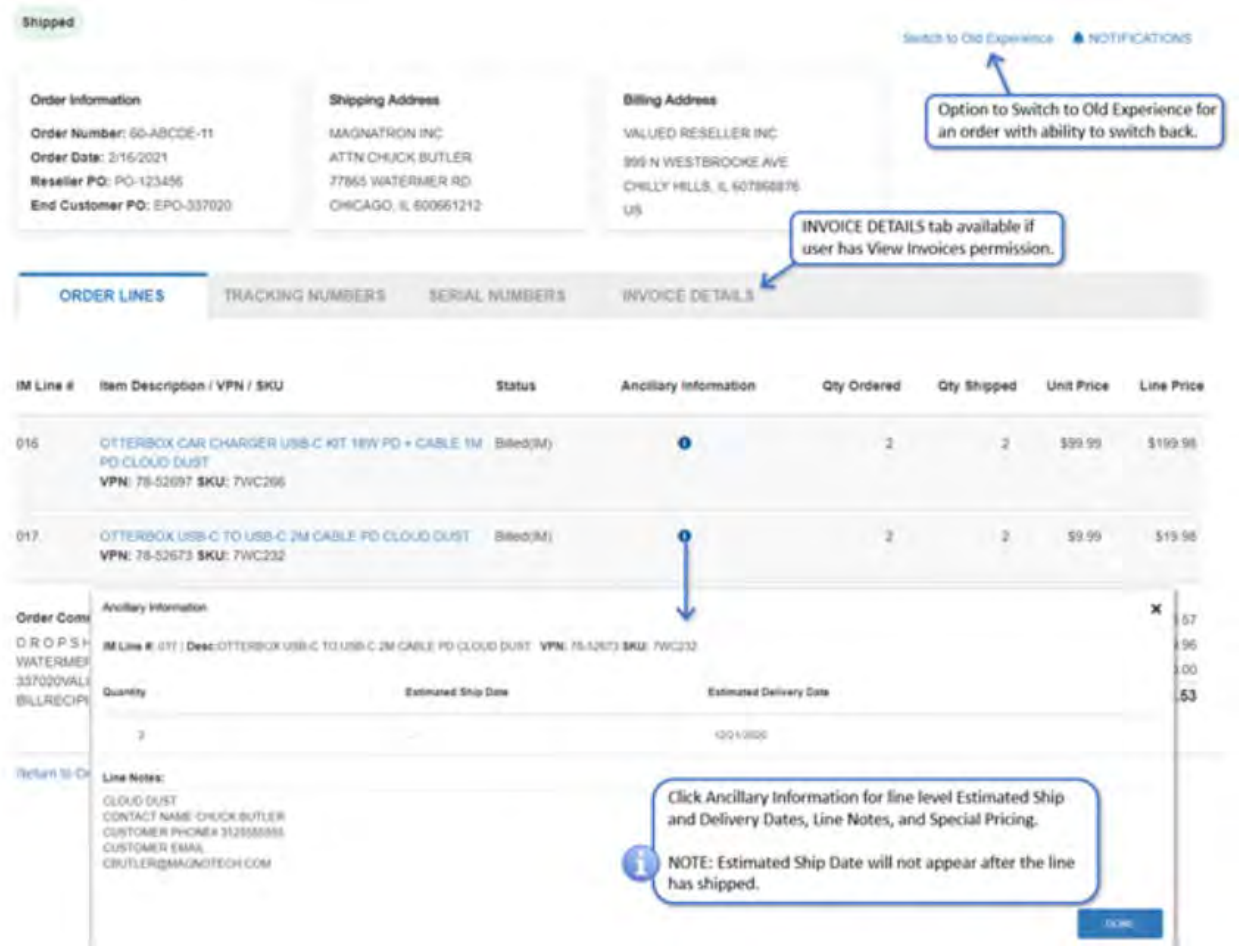
- PO numbers
- Addresses
- Status
- Use an existing order to create a new cart
- Line level order details
- Tracking information
- more

You can view changes in order status and set up notifications.

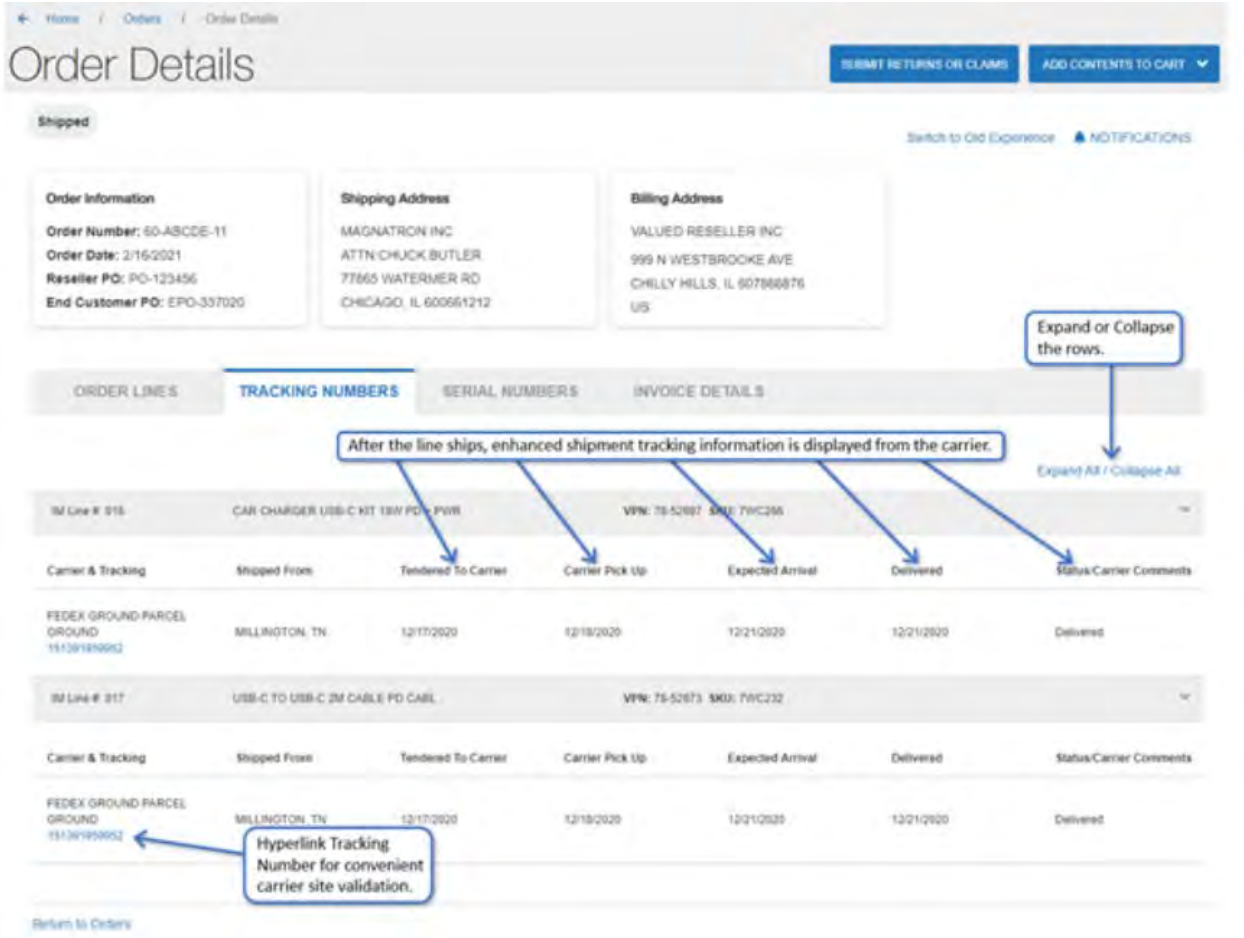
View Order Details

Use these steps to view order details:

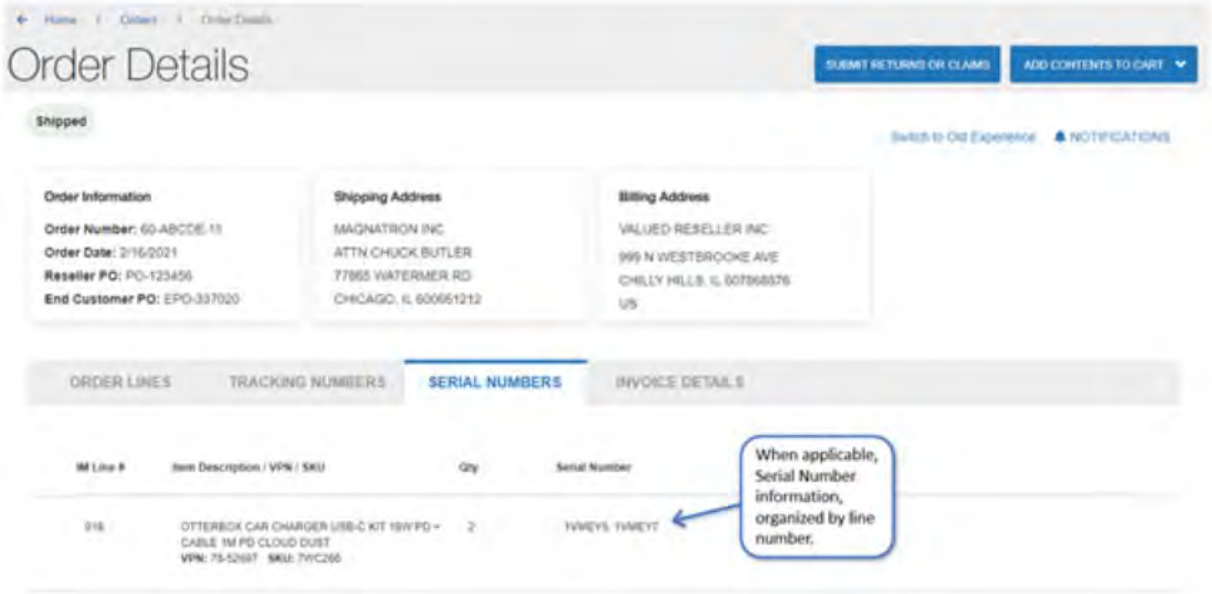
1. On the **Order List** screen, click any **IM Order#** to show **Order Details**.
   - Option to Switch to Old Experience
   - Access the Tab options for additional details
   - **ORDER LINES:**
     - Ancillary Information option for Line Notes, Special Pricing, and shipping estimates (when available)



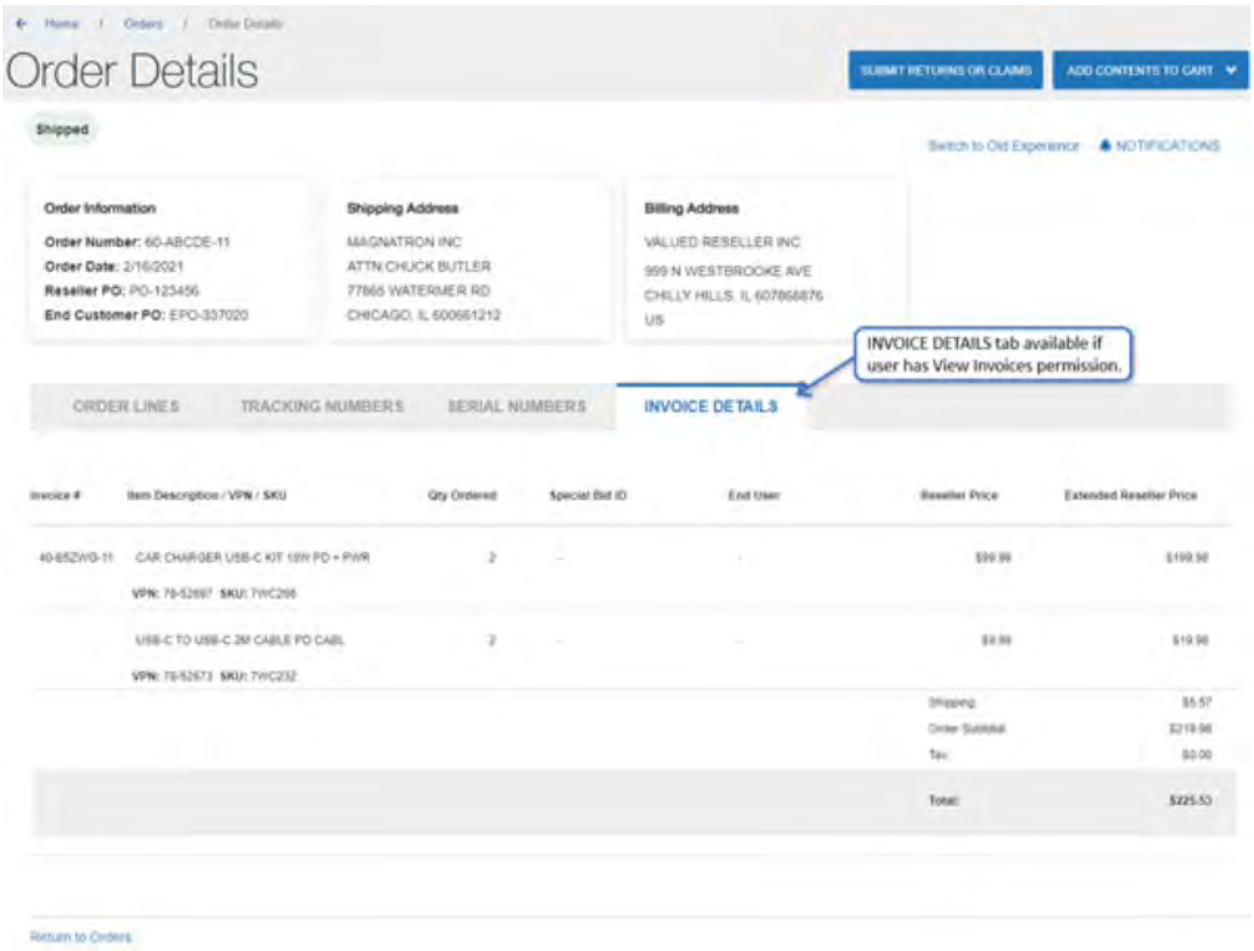
- **TRACKING NUMBERS for shipped items:**
  - Provides enhanced shipping information by tracking number, when this is available.
  - Includes Tendered to Carrier, Carrier Pickup, Expected Arrival, Delivered, Status
  - **Expand All / Collapse All** option



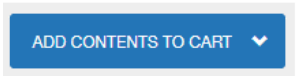
- **SERIAL NUMBERS:** Contains the SKU, VPN and serial numbers for each line item in the order, as available.



- **INVOICE DETAILS:**
  - Has a permission based access
  - Contains the Invoice #, SKU, VPN, Qty Ordered and pricing details for each line item in the order, as available.

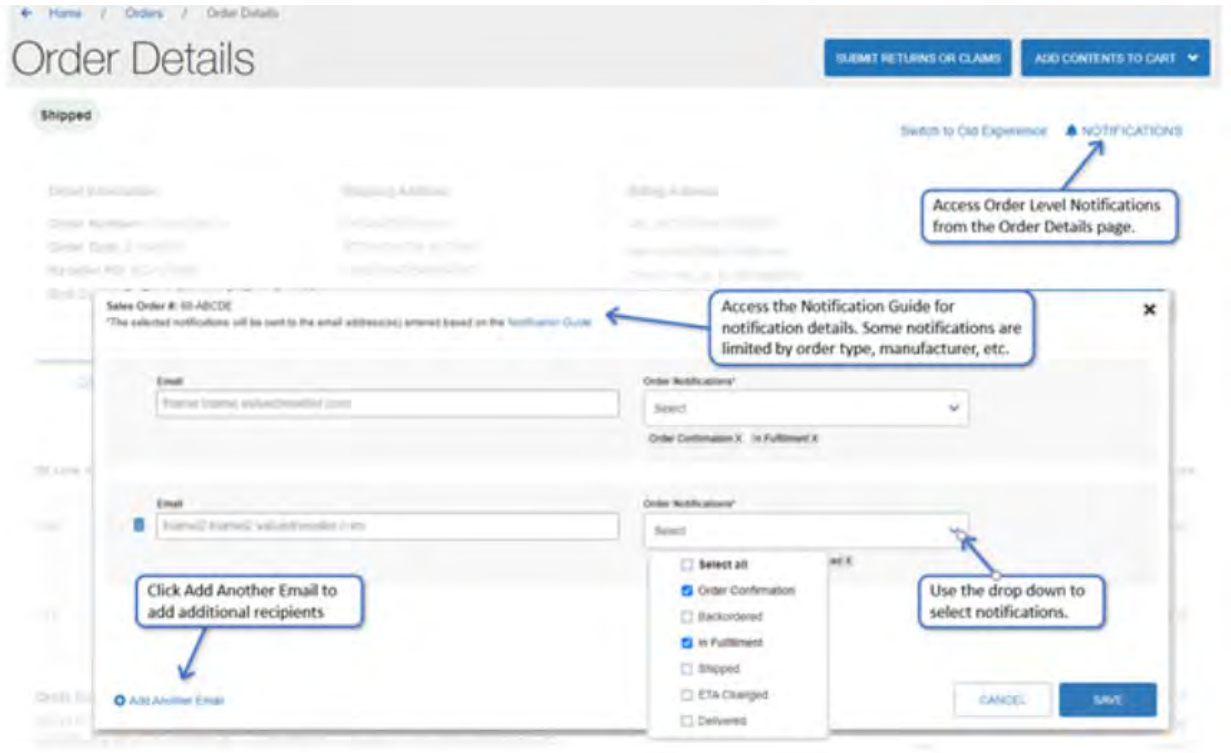


- **ADD CONTENTS TO CART**: Use this feature to copy all items in this order into the active cart. This is a convenient way to manage carts and orders if you often order the same products.



- **SUBMIT RETURNS OR CLAIMS**: Use this feature (when available) to navigate to the Returns Management page. Refer to Returns and RMA

- **NOTIFICATIONS**: You can set up or adjust notifications for any order:
  - Click **NOTIFICATION** from the **Order Details** page.
  - On the **Order Notifications** page, add categories of order notification, can add multiple emails, edit information and click **SAVE**.



2. Please click here for more information and a training document

Back to top

Invoice Gateway

The Invoice List screen provides transaction and payment history for your Ingram Micro account.

You can also get detailed invoice information by using our Invoice Gateway tool. Quick Start User Guide

This page contains topics to help you use invoice records:

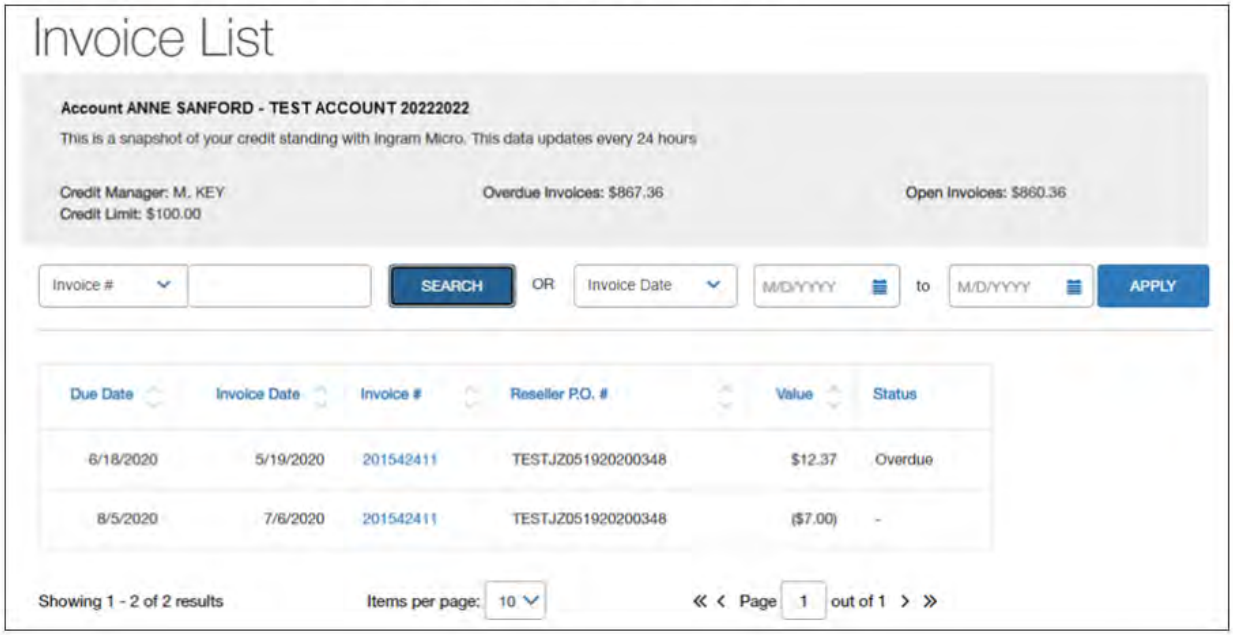
- View & Search Invoices
- View Invoice Details

View & Search Invoices

Use these steps to go to the invoices for your account.

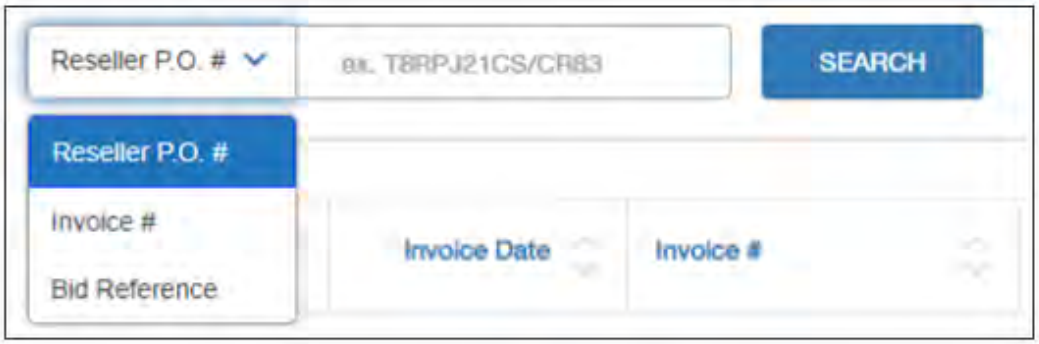
1. Click the **My Account** icon > **Invoice List**.

The **Invoice List** screen contains invoices you can search or sort in multiple ways.



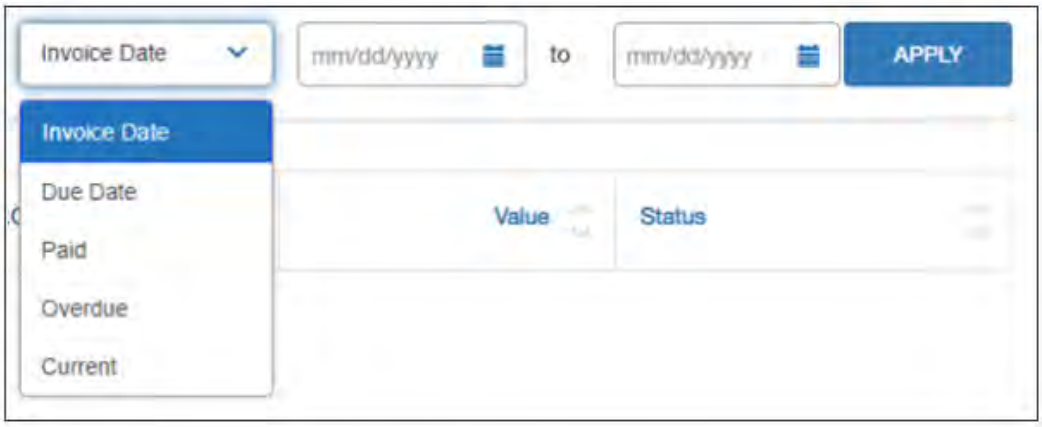
2. Search invoices by text string.

- Choose a search type from the drop-down menu options:
  - **Reseller P.O. #**
  - **Invoice #**
  - **Bid Reference**



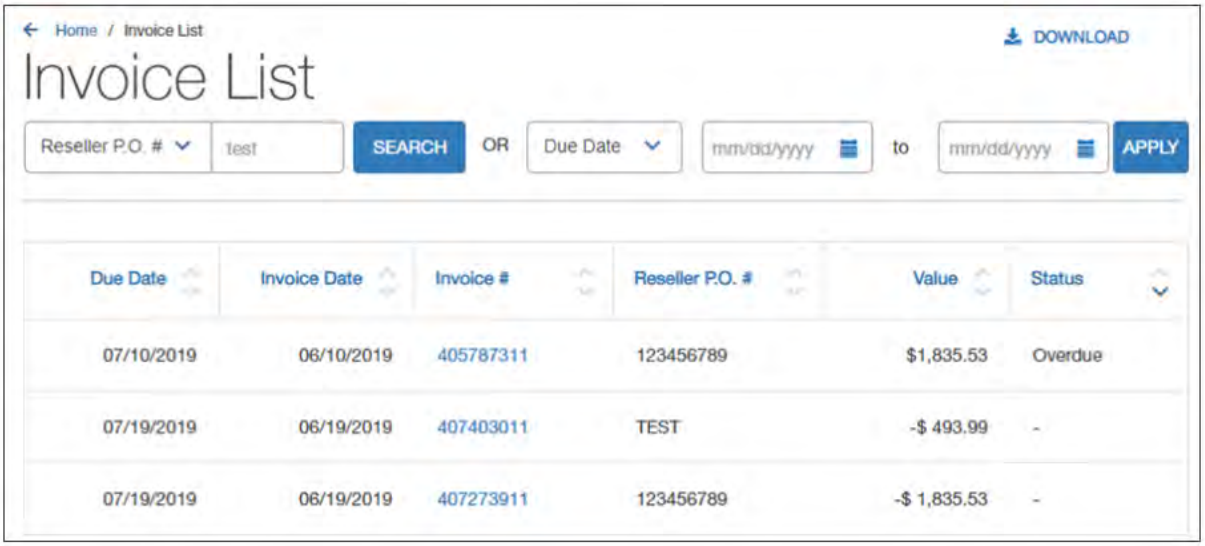
- Choose a search type, enter the text string, and click **SEARCH**.
  - The **Invoice List** screen displays any invoices that meet search criteria.
  - Sort invoices with step 4.

3. As an alternate method, search invoices by date range.
    - Choose a type of date range from the drop-down menu options:
        - Invoice Date
        - Due Date
        - Paid
        - Overdue
        - Current



    - Select a start and end date for the date range.
    - Click **APPLY**.
        - The **Invoice List** screen displays any invoices that meet search criteria.
        - Sort invoices with Step 4.

4. You can sort invoices by any column on the **Invoice List** screen.

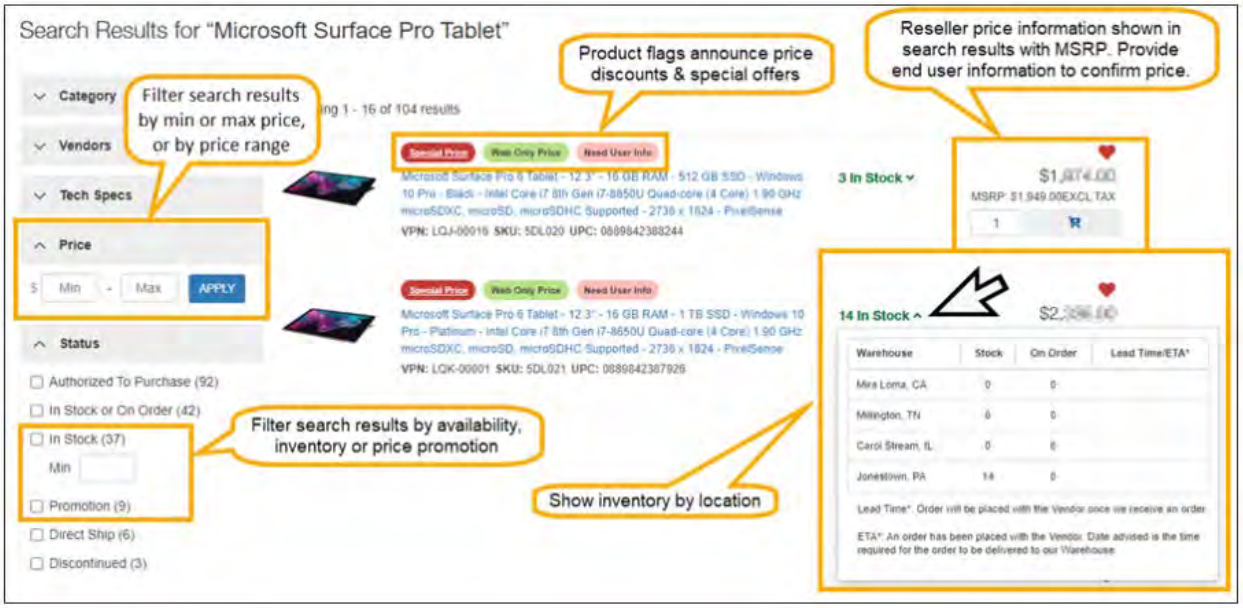


5. Sorting: Sort invoices by any column.
   - **DOWNLOAD**: Use this option to obtain a CSV spreadsheet file of invoices.

Back to top

Price & Availability

Team GSG offers several real-time price & availability features, as shown:



Product price & availability features:

- Product Price
  - Information is available on multiple screens
  - Price information can include:
    - MSRP
    - Reseller or dealer price
    - End user price
    - Quantity discounts and special price
    - Government or educational price
- Vendor Bids
  - Search & filter vendor bids from the vendor bid portal
  - View vendor bids from Product Details
  - View vendor bids from Cart
- Vendor Reporting
  - Search & view vendor offers & resources in this consolidated vendor resource portal
- Stock & Inventory
  - Information is available on multiple screens
  - Inventory shown by warehouse location
  - Products on order shown with lead-time

Is all work performed within the United States? Is work performed by employees, contractors, or sub-contractors. Please indicate the percentage performed by each group.

Yes, all the work will be performed within the United States. All the work will be performed by employees, contractors, and sub-contractors (employees 75%, contractors 15%, subcontractors 10%).

Indicate the level of certification and accreditation of your employees or contractors on the tools they use in the delivery of services.

GSG maintains a pool of extraordinary cybersecurity professionals. The quality of our team is peerless, having executed numerous programs of similar scope and complexity. Each of our proposed personnel have more than **10 years of experience** in providing cybersecurity and related services.

GSG's cybersecurity personnel have successfully completed more than 1,000 projects, including penetration testing, cybersecurity audits, cybersecurity assessments, vulnerability assessments, web application security assessments, risk assessments, etc. We have extensive experience with numerous IT and cybersecurity technologies such as HPE, Micro Focus, Splunk, IBM, Palo Alto, Fortinet, Cisco, AWS, Azure, etc. Our team is experienced in working within the NIST Cybersecurity Framework; Federal Risk and Authorization Management Program (FedRAMP); Payment Card Industry Data Security Standard (PCI–DSS); Open Web Application Security Project (OWASP); Center for Internet Security Critical Security Controls for Effective Cyber Defense; and other standards and practices.

GSG requires one or more of the following certifications for personnel implementing our cybersecurity services (not including account/project management and sales personnel):

- **CAP** — Certified Authorization Professional
- **CCIP** — Certified Core Impact Professional
- **CCSK** — Certificate of Cloud Security Knowledge
- **CGEIT** — Certified in the Governance of Enterprise IT
- **ISSAP** — Information Systems Security Architecture Professional
- **GIAC** — Global Information Assurance Certifications including (but not limited to):
  - **GSEC** — GIAC Security Essentials
  - **GCIH** — GIAC Certified Incident Handler

- **CHSE** — Certified HIPAA Security Expert
- **CISA** — Certified Information Systems Auditor
- **CISM** — Certified Information Security Manager
- **CEH** — Certified Ethical Hacker
- **CISSP** — Certified Information Systems Security Professional
- **CRISC** — Certified in Risk & Information Systems
- **CSX** — Cybersecurity Nexus
- **CSX–P** — CSX Cybersecurity Practitioner
  - **GPEN** — GIAC Penetration Tester
  - **GCIA** — GIAC Certified Intrusion Analyst
  - **GWAPT** — GIAC Web Application Penetration Tester
  - **GCFE** — GIAC Certified Forensic Examiner
  - **GCFA** — GIAC Certified Forensic Analyst
- **SANS–508** Advanced Forensics
- **SANS–572** Advanced Network Forensics

Where services are to be supplied – what are the choices of license model. Does the customer own the software license or the vendor? Is there a choice?

Services will be supplied to fulfill all the different demands of NCPA. As there are multiple products and services are available through our teaming partner Ingrma Micro, there would be various choices of license model available to the NCPA. Ownership of software licenses depends upon the product/service being provided. Most products have different licensing models available.

Who owns the security data artifacts and where are they held? What is the process of supplying the data to the customer at termination of services?

Security data artifacts reside on the server (e.g., syslog/standalone/monitoring server). These data artifacts reside in system registry keys, files, timestamps, and in the form of event logs. All data artifacts are the property of the client. The service level agreement, contracts clauses and data processing agreement will manage the customer data disposition after termination of services.

Describe your company's Customer Service Department (hours of operation, number of service centers, etc.)

Team GSG has representatives available in multiple time zones. Therefore, the customer service is available from GSG and team 24 x 7. In today's business environment, protecting your organization and its data against the fast-changing landscape of next generation threats is mission critical. Today, security-conscious enterprises and federal government agencies choose Team GSG and Mandiant for industry-leading protection against these next generation threats. They also need technical support so they can maximize the value of this infrastructure — and quickly get help to keep systems up and running to protect against today's stealthy web, email, and file sharing threats.

Team GSG Support is available to all customers who have purchased the following Team GSG and Mandiant products and solutions: Team GSG Helix, Team GSG Network Security (including NX, Cloud MVX, and SmartVision products and subscriptions), Team GSG Email Security (including EX and ETP), Team GSG Endpoint Security (including HX), Team GSG AX, Team GSG File Analytics (FX), Team GSG Detection on Demand, Team GSG Cloudvisory, Team GSG Network Forensics (PX), Team GSG Central Management Series, Team GSG Threat Analytics, Mandiant Automated Defense (fka Respond Software), Mandiant Security Validation (fka Verodin) and Validation on Demand, and Mandiant Intelligence ('Supported Offerings').

Ingram Micro support is available for ALL products purchased through their portal.

Team GSG Support Principles

Team GSG Support provides responsive, high-quality services, striving to achieve the highest level of customer satisfaction by:

- Providing timely and knowledgeable responses

- Helping protect the customer's investment
- Meeting changing market demands for new features, products, and services
- Providing information to customers to assist in decision making — for example, concerning system upgrades, system configurations, etc.

For most Team GSG products, four Support Programs are offered to meet customer needs. In addition, spare parts are available for quick turnaround hardware replacements, and a non-returnable disk drive service allows customers to keep disk drives in the event of a drive failure.

Team GSG Support Programs

The key to our support programs is flexibility — we offer a combination that meets today's business needs to ensure world class threat protection and mission critical coverage. For NCPA, Team GSG is proposing our Government Support Program.

For customers who have purchased Team GSG Helix, Team GSG Network Security (including NX, Cloud MVX, and SmartVision products and subscriptions), Team GSG Email Security (including EX and ETP), Team GSG Endpoint Security (including HX), Team GSG AX, Team GSG File Analytics (FX), Team GSG Detection on Demand, Team GSG Cloudvisory, Team GSG Network Forensics (PX), Team GSG Central Management Series, Team GSG Threat Analytics, Mandiant Automated Defense (fka Respond Software), Mandiant Security Validation and Validation on Demand (fka Verodin) and Mandiant Intelligence, Team GSG offers four support programs on an annual or multiyear basis, as shown below.

[1] Available in select countries — contact your Team GSG account representative for details.

[2] Provided RMA is issued prior to local business day cutoff time and no external-to-Team GSG circumstances prevent delivery.

[3] Available for select Team GSG Products. Customers who purchase 1-way DTI Content Delivery may opt out of Proactive Support by notifying Team GSG Customer Support.

[4] Not applicable to Mandiant Threat Intelligence Offerings, Mandiant Security Validation, Validation on Demand, or Mandiant Automated Defense.

Only entitlements listed above for Platinum Support are available for Mandiant Automated Defense, Mandiant Threat Intelligence, Mandiant Security Validation, and Validation on Demand purchases.

Government Support Program

The Government Support Program covers hardware, software, and subscription support for Supported Offerings, and includes:

- Assistance via multiple channels: Live chat, web, phone, and email support 24/7/365 for up to 15 designated contacts
- Target Initial Response Times as detailed in table below
- Immediate escalation to Advanced Level Three Engineering Support for Severity One cases, provided case is phoned through to align customer and Team GSG resources
- Maintenance releases for security efficacy and other recommended software bugfixes, as well as new releases for general software updates and non-chargeable enhancements to assure systems contain the latest Team GSG updates and stay compatible with evolving technology
- Emergency fixes, tested and verified by Team GSG engineering, for Severity One issues
- Return of defective products subject to the limited warranty

- Advance replacement of defective hardware, as described below
- Access to the secure Team GSG Support Portal, community, and knowledge base, which includes:
  - A Support Portal for opening and updating support cases for your designated contacts
  - A community to find and share solutions with Team GSG users around the world
  - A knowledge base of known issues and articles
  - Online documentation
  - Patch/update information
  - Field notices
  - Cloud service status

Initial Response Times

Team GSG will use reasonable efforts to respond to requests for support as detailed below:

Severity	Impact	Target Initial Response Time
One	• Product rendered unavailable or unresponsive, requires constant restarting, or results in irretrievable corruption or loss of data • Major application not functioning • Device not scanning, or device blocking traffic • Requires immediate fix	[redacted]
Two	• Sub-component of a major application not functioning as documented • Services degraded • Major performance degradation	[redacted]
Three	• Minor application not functioning as documented	[redacted]
Four	• General usage question • General information requests • Feature requests	[redacted]

Green Initiatives

At GSG, we are constantly aiming to minimize our impact on the environment. We stress reduction of waste generated by employees and encourage recycling, energy conservation, and water conservation efforts, such as providing employees with filtered water stations to reduce the use of bottled water.

Every printer has a paper recycling box next to it rather than a wastebasket. We purchase supplies that contain a high percentage of post-consumer recycled content. When the building is not occupied, we do not run lighting.

To further reduce the use of fuel and energy required for document delivery, GSG also encourages the use of Scan-on-Demand. When a client needs a document, it can be scanned and delivered electronically, eliminating the need for a physical delivery, further reducing the use of fuel and release of emissions into the environment. Many of our technology offerings are designed specifically to reduce the amount of waste material and energy use that accompanies maintenance and storage of physical documents.

Vendor Certifications (if applicable)

GSG's Michigan Certificate of Good Standing

This is to Certify That

GLOBAL SOLUTIONS GROUP, INC.

was validly incorporated on May 1 , 2003 as a Michigan DOMESTIC PROFIT CORPORATION, and said corporation is validly in existence under the laws of this state.

This certificate is issued pursuant to the provisions of 1972 PA 284 to attest to the fact that the corporation is in good standing in Michigan as of this date and is duly authorized to transact business and for no other purpose.

This certificate is in due form, made by me as the proper officer, and is entitled to have full faith and credit given it in every court and office within the United States.

In testimony whereof, I have hereunto set my hand, in the City of Lansing, this 31st day of October , 2018.

Julia Dale, Director

Corporations, Securities & Commercial Licensing Bureau

Sent by electronic transmission

Certificate Number: 18108936150

Verify this certificate at: URL to eCertificate Verification Search http://www.michigan.gov/corpverifycertificate.

GSG's MBE Certificate

THIS CERTIFIES THAT

Global Solutions Group, Inc.

NMSDC
National Minority Supplier Development Council

* Nationally certified by the: **MICHIGAN MINORITY SUPPLIER DEVELOPMENT COUNCIL**

*NAICS Code(s): 541511; 541512; 541611; 561110; 561320; 561410; 541519; 561621

* Description of their product/services as defined by the North American Industry Classification System (NAICS)

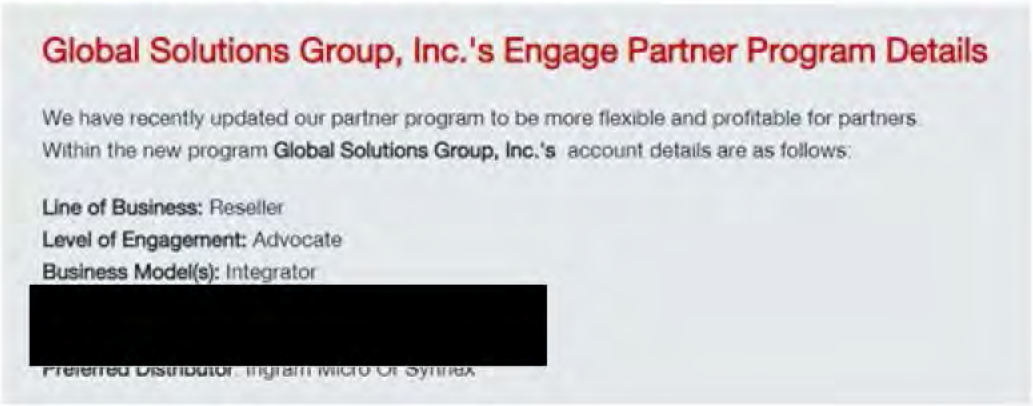
09/28/2021		MI03275
Issued Date		**Certificate Number**
	NMSDC CEO and President	
10/01/2022		Michelle Sourie Robinson
Expiration Date		**Michelle Sourie Robinson, President & CEO**

By using your password (NMSDC issued only), authorized users may log into NMSDC Central to view the entire profile: http://nmsdc.org

Certify. Develop. Connect. Advocate.

* MBEs certified by an Affiliate of the National Minority Supplier Development Council, Inc.®

GSG's Fortinet Engage Partner Program details:



Global Solutions Group, Inc.'s Engage Partner Program Details

We have recently updated our partner program to be more flexible and profitable for partners.
Within the new program **Global Solutions Group, Inc.'s** account details are as follows:

Line of Business: Reseller
Level of Engagement: Advocate
Business Model(s): Integrator
[redacted]
Preferred Distributor: Ingram Micro or Synnex

The following is our partner Ingram Micro's Fortinet Certificate of Authorized Distributor:

GSG is an authorized reseller of all Ingram Micro products.

FORTINET

Certificate of Authorized Distributor

Date: 02/10/2021

Fortinet, Inc. operates through a channel of independent distributors and resellers. Therefore, Fortinet hereby confirms that: Ingram Micro US

Having its registered place of business at:
1600 E ST ANDREW PLACE, SANTA ANA, CA 92705, United States;

is currently an authorized Distributor and is currently authorized throughout US to sell Fortinet products as a partner with the following designations:

- Level of Engagement:

This certificate is issued as of the date shown above, and is valid for 180 days from this date.

Provided the FortiPartner identified above has purchased applicable support services from Fortinet and the applicable support services have been effectively registered and contracted with Fortinet, Fortinet agrees and undertakes that Fortinet would provide support for the applicable Fortinet products according to the terms of the support agreement, available at https://support.fortinet.com. Fortinet Products are shipped subject to the terms of its then-current End User License Agreement, available at http://www.fortinet.com/doc/legal/EULA.pdf, which sets forth Fortinet's warranty.

[redacted]

Manufacturer Confirmation

Samantha Symonds
Vice President of Legal and Compliance, Americas

FORTINET, INC.
899 Kifer Road
Sunnyvale, CA 94086

[redacted]

GSG Letters of Authorization

Gigamon

www.gigamon.com

February 11, 2021

To whom it may concern,

As of the date of this letter, Gigamon Inc., located at 3300 Olcott Street, Santa Clara, CA 95054 ("Gigamon"), confirms that **Global Solutions Group, Inc.**, located at 25900 Greenfield Road, Ste. 220 Oak Park, Michigan, , United States ("Reseller Country"), is authorized to resell Gigamon hardware, on premise software, and product support maintenance, per the reseller agreement between Gigamon and **Global Solutions Group, Inc.**, dated 2/9/2021, to end customer entities located in the Reseller Country.

Should you have any questions, please do not hesitate to ask.

Sincerely,

[redacted]

Vicon Security

VICON

Ref: Authorized Reseller Acknowledgement

To whom it may concern:

This is a notification letter verifying that **Global Solutions Group, Inc.** is a Vicon Authorized Reseller (VAR) and Dealer/Integrator. **Global Solutions Group, Inc.** is trained and certified to install and service Vicon systems and components.

The quality of the performance by the installing dealer affects all aspects of the overall satisfaction of the end-user with their video surveillance system. As a VAR and Dealer **Global Solutions Group, Inc.** will ensure a timely, professional, and operation compliant installation involving little or no end-user intervention through project installation and completion.

Vicon's commitment to providing quality installations does not end with the qualification and selection process. VARs and Dealers admitted to the program will be required to maintain the standards for Certification on an ongoing basis.

If you have any questions, comments, or concerns, please contact Vicon's South West Regional Manager [redacted]

Sincerely,

[redacted]

Microsoft

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

11/18/2021

To whom it may concern:

I hereby confirm that Global Solutions Group, Inc. has satisfied the requirements for demonstrating and validating their technical capabilities in the Microsoft Partner Network program.

Global Solutions Group, Inc. (MPNID: 3955544)
25900 Greenfield Road
Oak Park, MI - 48237
United States

Competencies: Demonstrate technical capabilities in Microsoft products or technologies.

- Gold Collaboration and Content (Expires on 11/29/2021)

Global Solutions Group, Inc. is currently doing business with Microsoft in the following locations:

- Global Solutions Group, Inc., US, Oak Park (Oak Park) (MPNID: 3955545)

[redacted]

Mandiant

DocuSign Envelope ID: DAE1E4DC-207D-402A-8C4A-F92A93D5BAD5

MANDIANT
YOUR CYBERSECURITY ADVANTAGE

October 24, 2021

Re: Letter of Authorization for Global Solutions Group, Inc.

To Whom It May Concern:

This letter serves as confirmation that Global Solutions Group, Inc. ("GlobalSol") is an active, authorized Mandiant, Inc. ("Mandiant") silver level partner in good standing. Pursuant to the Reseller Certification Agreement entered into by the GlobalSol and Mandiant, GlobalSol is authorized to distribute, resell, or otherwise provide Mandiant solutions within the United States, including the US. Federal Government and U.S. state and local government entities, K-12 educational entities, and institutions of higher education, State Government, Local Government, and Education.

[redacted]

[redacted]

info@mandiant.com

FireEye

October 24, 2021

Re: Letter of Authorization for Global Solutions Group, Inc.

To Whom It May Concern:

This letter serves as confirmation that Global Solutions Group, Inc. ("GlobalSol") is an active, authorized FireEye Security Holdings US LLC ("FSH") silver level partner in good standing. Pursuant to the Reseller Certification Agreement entered into by the GlobalSol and FSH, GlobalSol is authorized to distribute, resell, or otherwise provide FSH offerings within the United States, including the US. Federal Government and U.S. state and local government entities, K-12 educational entities, and institutions of higher education, State Government, Local Government, and Education.

[redacted]

[redacted]

Tab 5 – Products and Services

The following table demonstrate our overview of products and services offered to NCPA:

Service Categories	Sub-categories	Tool / Solution Team Partner(s)
Identify — Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities	Asset Management	Saffire Tools
	Asset Discovery	Saffire Tools
	Business Environment	SWOT
	Governance	Tenable, Jumio, IBM, Fortinet
	Risk Management	Upguard, Cisco
	Risk Management Strategy	Upguard
	Vulnerability Scanning and Management	Tenable, Acronic, Arcserve
	Supply Chain Risk Management	Splunk
Protect — Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services	Identity Management	Azure AD, Beyond Trust, Jumio
	Authentication & Access Control	Cyberarc, Beyond Trust
	Multi-factor Authentication (MFA)	RSA, Symantec, Azure
	Awareness & Training	Knowbe4, Code42
	Data Security	Imperva, ArcServe, Tenable
	Information Protection & Procedures	Fortinet
	Maintenance	Fortinet
	Protective Technology	Fortinet, Gigamon
Detect — Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Anomalies & Events	Cobalt
	Security Continuous Monitoring	Alient Vault, Microsoft, Gigamon, IBM, Tenable
	Detection Process	Cobalt
	Log and Event Correlation (SIEM)	IBM QRadar, Splunk, Gigamon, Fortinet, Alertlogin, FireEye
	User Behavioral Analytics (SIEM)	Cobalt, Fortinet
Respond — Develop and implement the appropriate activities to respond to detected cybersecurity events	Response Planning	ServiceNow, Jira, FireEye
	Data Enrichment	ServiceNow
	Communication	ServiceNow, Jira

	Analysis	ServiceNow, Jira, FireEye
	Mitigation	SharePoint
	Automated Response	ServiceNow, Jira, FireEye
	Improvements	ServiceNow, Jira
Recover — Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Recover Planning	Acronic, Arcserve
	Forensic Investigation	Acronic, Gigamon
	Findings Report	ServiceNow, Jira
	Improvements	ServiceNow, Jira
	Communications	ServiceNow, Jira

Services Related to the Scope of Work

GSG understands the increasing emphasis for heightened security throughout the Federal Government, and we are currently executing a similarly high-level cyber security contract for the [redacted]. We are currently developing new security methodology and assessment standards for multiple agencies within the Department. We have developed a technical approach that can be customized to meet the specific requirements of any agency while still ensuring full compliance with the National Institute of Standards and Technology (NIST) Risk Management Framework, FISMA requirements and privacy protection concerns. Having thoroughly reviewed the issued RFQ and any associated documents, we feel that GSG can offer the NCPA a highly effective cyber security solution.

Perform Security Analysis.

GSG's Security Review methodology includes the following steps:

- Review of latest security reports;
- Analysis of current IT network, information flow according to business requirements and points of access to information;
- Analysis of current security controls and procedures for various security management areas;
- Analysis of current policies and procedures for both IT personnel and end users
- Analysis existing network security architecture, including topology/ configuration, and security components/features
- Provide gap analysis or prioritized recommendations on network architecture and placement of security controls. The in-depth principles used to ensure security controls are applied for information transport, and access to networks, hosts, applications and data. The outcome will be a recommendation that has the proper combination of the security services at each level to deliver a cohesive security posture that reflects the enterprise's risk management objectives. The security controls and procedures of various security management areas will be addressed, such as Threat Management, Vulnerability Management, Identity Management and Change Management
- Provide assessment of the existing security controls and prioritized recommendations on improvements and/or additional controls to meet specified security policies
- Provide assessment and prioritized recommendations on security procedures

- Provide an evaluation of the security architecture for performance, scalability, reliability and manageability

Developing, Validating, and Processing Risk Management Framework Authorization Packages

The Risk Management Framework (RMF) is the unified information security framework for the entire federal government. RMF was established by the National Institute for Standards and Technology (NIST), in partnership with the Department of Defense, the Office of the Director of National Intelligence (ODNI) and the Committee on National Security Systems (CNSS) to develop a common information security framework for the federal government and its contractors in making risk-based decisions. The RMF has identified the following activities, which can be applied to both new and legacy systems:

Categorize – Classify and label the information processed, stored, and shared, and the systems that are used; this is done based on an impact analysis

Select – Review the categorization and select baseline security controls; revise and add to the security control baseline as necessary, based on organization assessment of risk and local conditions

Implement – Instill the security controls and integrate with legacy systems; document how the controls are arrayed within the system and their effects on the environment

Assess – Evaluate the security controls to determine whether they are implemented correctly, and their quality and effectiveness

Authorize – top management tests and approves the secured system based on the accepted risk appetite to operations and assets (how much risk the organization is willing to tolerate). Management also considers the system's operational impact on individuals, other organizations, and the US. It will identify how much risk is still present, and either authorize it or decide on changes needed.

Monitor – Set up an ongoing monitoring and assessment schedule for security controls to measure effectiveness. Document system or operation adjustments, and include impact analyses of changes made, Report findings to information security officials

External Network Vulnerability Assessment and Penetration Testing

GSG's External Network Vulnerability Assessment identifies the key strengths and weaknesses of the County's current environment, allowing you to see how it would handle various types of cyber-attacks. Once we have assessed your system for vulnerabilities, we conduct simulated attacks where we behave like the world's most sophisticated cyber-intruder to determine how those vulnerabilities could be exploited. Using the results, we develop a remediation strategy that will help the County mitigate the risk of falling victim to authentic cyber intruders. GSG delivers public-facing network services that could provide a point of entry to unauthorized attackers through the successful exploitation of identified vulnerabilities. Performing assessments against the external network vulnerability can help an organization:

- ✓ Confirm publicly available networks / systems and the applications running on those systems;
- ✓ Fulfill requirements of applicable regulations and / or compliance standards;

- ✓ Validate / assess the effectiveness of existing security controls;
- ✓ Identify / assess the impact of network weaknesses before a malicious attacker does;
- ✓ Assess the adequacy of intrusion detection and response systems; and
- ✓ Gain actionable recommendations designed to mitigate discovered vulnerabilities.

Our External Vulnerability Assessment testing methodology is continuously engineered to meet evolving best practices and is informed by several standardized approaches. Each engagement is customized to meet unique goals and objectives, therefore the specific elements of our methodology that are leveraged is contingent upon the level of testing and defined scope.

The following is an accounting of the potential testing phases and their respective individual elements:

Footprint Reconnaissance / Analysis

This step involves searching various publicly available sources for detailed company-specific information. This allows us to identify target systems and provides information that may prove useful in an attack.

System, Service, and Vulnerability Identification

Here we take a more focused look at the devices, servers, and Internet-facing applications. We use a variety of specialized security tools to identify the architecture and vulnerabilities. The goal is to identify systems / devices that respond to authorized and unauthorized requests, the services / applications that those systems are providing, and inherent and/or potential vulnerabilities.

Exploitation

This is the attempt to gain unauthorized access to systems and / or information utilizing the vulnerabilities identified in the previous phase. This task is customized based upon the findings of the engagement. GSG's approach is to exploit the network vulnerability and gain access to systems / information; once access is obtained, GSG will report the finding to the the County so the method of access can be remediated promptly. If requested by the the County, GSG can attempt to pivot the attacks towards internal machines; however, our general approach is to report the finding and move on in an attempt to find additional external vulnerabilities.

Reporting

In this final phase of the engagement. GSG will generate an executive summary and a technical report that explains the findings, includes visuals/screenshots, provides customized remediation recommendations, and, if available, includes details on repeating the attack scenario.

GSG's cybersecurity professionals bring highly skilled expertise to each unique engagement through specialized training in security testing disciplines. Continuous education is a fundamental element of ensuring quality testing and our personnel maintain several professional credentials as well.

Internal Network Vulnerability Assessment and Penetration Testing

GSG's Internal Network Vulnerability Assessment services are designed to assess your network security from the inside. Vulnerabilities can arise due to misconfigured hardware, out of date software or unpatched systems/software. Attacks can come from a malicious insider, viruses, malware, or unintentional attacks such as an accidental deletion of sensitive data. The objective of an

Internal Vulnerability Assessment is to safeguard the network's assets that could be exploited to interfere with the confidentiality, availability, and integrity of your network.

Our security experts provide an insightful review of the state of all internal network assets including vulnerabilities, misconfigurations, and other health indicators. Since 2000, GSG has been leveraging our security professionals who have extensive experience reviewing real-world exploits daily.

GSG's Internal Network Vulnerability Assessment is a hands-on, privileged security inspection consisting of two components. First, we look at the configuration of systems to evaluate the strengths and weaknesses of the County information system's design and technical / operational controls. Then we run a vulnerability scan on internal network to identify vulnerabilities that are specific to your system and devices. We use the credentials of domain administrators, which allows us to look at things like domain registries and patches.

Through the Assessment, we will:

- ✓ Document your global network security settings and configurations.
- ✓ Document the relative strengths and weaknesses of your current technical and operational controls.
- ✓ Assign compliance ratings of system configuration and settings in accordance with industry standard and regulatory best practices, including FFIEC, NCUA, and CMS guidelines, the National Security Agency Gold Standard, National Institute of Standards and Technology guidance, ISO 27002 standards, and relevant vendor recommendations.
- ✓ Identify system/device-specific vulnerabilities using the Department of Homeland Security Common Vulnerabilities and Exposures (CVE) database.
- ✓ Provide specific, detailed remediation recommendations.

GSG follows the following methodology for Internal Vulnerability Assessments:

Data Collection

GSG's Security expert will meet the County onsite to perform data collection. We conduct the configuration review using automated and manual open source, commercial and proprietary tools, interviews, and observation techniques. Administrative credentials are required to perform the Configuration Assessment.

We conduct the Vulnerability Assessment using a licensed commercial vulnerability scanner that supports a wide range of network devices, operating systems, databases, and applications. While administrative credentials are optional for the vulnerability scans, we encourage using them to scan Microsoft Windows environments because the results will be more accurate and will better expose the system's vulnerabilities.

Data Analysis

Our experts perform the Data Analysis Phase of the Assessment offsite by reviewing the data we have collected. In the Configuration Assessment Analysis, we compare each system and assign compliance ratings in accordance with industry standard and regulatory best practices. In the Vulnerability Assessment Analysis, we review the results of the vulnerability scans to ensure that the most relevant information is included in a clear and concise manner.

Reviewing our Findings

Once we have analyzed the data, we will schedule a meeting with the County to review the results with the County systematically.

The Internal Vulnerability Assessment report includes:

- ✓ A summary of the findings presented in an executive report in PDF.

- ✓ A corresponding interactive HTML report providing the details for each of the Assessment categories, as well as the device-specific vulnerabilities.
- ✓ An action plan detailing our recommended remediation activities.

Malware Infection Scanning and Evaluation

GSG evaluate**s** IT environment**s** to determine the extent of malware infection. We provided forensic analysis of infected devices to determine what data had been exposed, and re-imaged infected workstations. We also ensured that all workstations and servers were patched, and that the antivirus was operating correctly, and updated with the latest signature files and ensured that the scan engine was updated.

Deliverables:

- Assurance the environment is free of malware
- All operating systems are patched
- All workstations and servers have operational and up-to-date antivirus.

Tab 8 – Value-Added Products and Services

There are an estimated 3.5 million unfilled cybersecurity positions forecasted by 2021, and research suggests it's only getting worse. Insufficient and underskilled staff increase team workload, leading to burnout, attrition, and increased business risk. With security teams devoting so much time to acquiring cybersecurity expertise, critical activities such as strategic planning, threat hunting, and skills training are often deprioritized.

Rethink your approach to acquiring cybersecurity expertise. Instead of using your budget to hire a single expert for one role, you could have ad hoc access to a diverse set of cybersecurity capabilities, skillsets, and functions.

Mandiant Expertise On Demand from FireEye is an annual subscription that extends your security operations capabilities and capacity with flexible access to a wide range of industry recognized Mandiant security skills, experience and knowledge. This unique service can help reduce the business and management risks associated with hiring, training, and retaining cybersecurity talent by providing the expertise you need, when you need it.

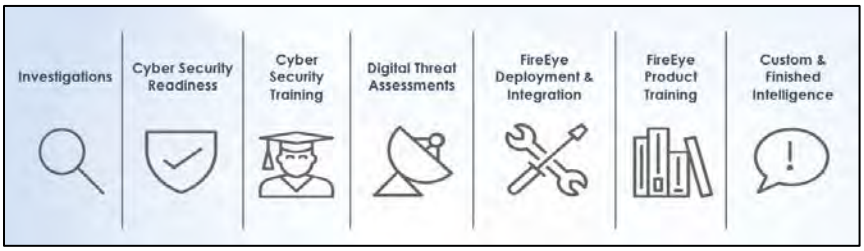
Introducing Expertise On Demand (EOD)

GSG has a strategic partnership with FireEye. FireEye's Expertise On Demand is an annual subscription that provides flexible access to FireEye's industry-recognized security expertise and threat intelligence using prepaid units. Existing prepaid units can be exchanged for services, and additional units may be purchased any time during the subscription. Our flexible consumption model provides a unique option for extending your security operations capabilities with the expertise you need when you need it most.

What You Get

- **Daily News Analysis** provides a daily email summary highlighting cyber threats observed or reported on by public resources including analysis of recent threat activity by FireEye analysts. The analysis provides an assessment of the reporting accuracy. The judgments are: On-Target, Off-Target, Judgment Withheld.
- **Quarterly Threat Briefings** are generally restricted to FireEye Threat Intelligence customers. The briefings inform you of global threat activity trends.
- **Incident Response Retainer** terms are included for all Expertise On Demand customers to help resolve the impacts of cyber breaches. The retainer helps accelerate incident response by proactively establishing contractual terms before an incident occurs. An optional Service-Level Agreement is available for additional units.
- **Ask an Analyst** provides access to FireEye's elite intelligence analysts and other experts, through email, chat, or Helix to provide deeper context and analysis in response to a customer's question. The questions can be related to the customer's cybersecurity posture or threat landscape, including (but not limited to) malicious actors or campaigns, specific vulnerabilities or threats, or alert investigations. See Figure 1 for examples of questions you can ask through Expertise On Demand.

Full-Service Portfolio — NCPA can also use Expertise On Demand units to gain access to FireEye's full-service portfolio of consulting, training, and intelligence services (see Figure 2). The portfolio includes fixed-scope services such as tabletop exercises, security operations training courses, intelligence capability development workshops, and all our custom-scoped FireEye Mandiant strategic services.



For a complete list of services available through Expertise On Demand, please see the Service Description.

The following are example use cases for an Expertise On Demand subscription:

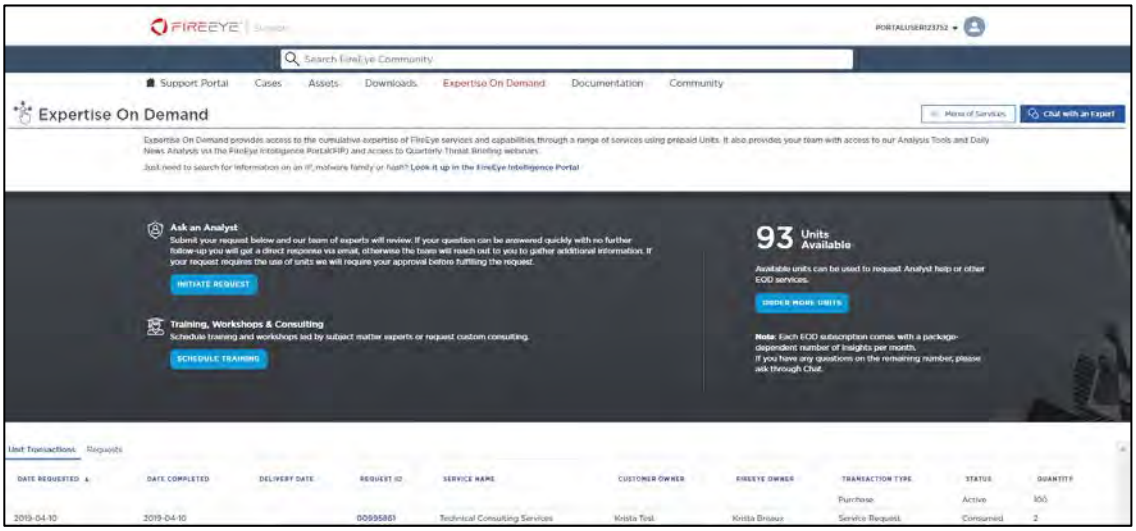
- **Accelerate Incident Investigation** — Gain insight into existing incidents, understand what FireEye knows about likely threats and backstop their team with intelligence analysts.
- **Increase Adversary Awareness** — Keep pace with threat landscape and prioritize response with Daily News Analysis of both threat-making headlines and activity FireEye analysts have observed in the wild.
- **Drive Proactive Hunting** — Design hunting missions based on who may be targeting your organization and likely attacker intent, techniques, and tools.
- **Accelerate Incident Response** — Gain the assurance of having Mandiant on standby should a breach occur.
- **Inform Security Program Strategy** — Align program investment and resource capabilities based on threats targeting specific industries.
- **Enhance Security Programs** — Identify program gaps and next steps via tabletop exercises that evaluate your team's skills, tools, and processes.
- **Upskill Security Teams** — Enhance your security team's skills with practitioner-led training on threat analysis, hunting, and incident investigation and response.

How It Works

Expertise On Demand can be purchased standalone or as a curated product-plus-expertise pairing to help accelerate your success with FireEye products. Expertise On Demand can also be paired effectively with non-FireEye technologies and services.

Based on your organization's specific needs and priorities, you can plan out your services to support a specific initiative, reserve services and investigations to secure against a future need, or a mix of both.

When planned (or needed), simply engage with our experts through the various means available to subscribers, including the Expertise On Demand Customer Portal, via email, or through the chat.



You can adjust your services as your security operation changes — subscribers can purchase additional services at any time.

Shortly after purchasing Expertise On Demand, subscribers receive a welcome email containing:

- Instructions for accessing the Expertise On Demand portal
- A summary of purchased entitlements
- Instructions for requesting Expertise On Demand services

Benefits of FireEye Expertise On Demand

Expertise On Demand provides access to the cumulative expertise of FireEye services and capabilities through a range of fixed- and custom-scope services using prepaid units. Table 1 summarizes the features and associated benefits of Expertise on Demand:

	Description	Benefits
Ask an Analyst	• Ask FireEye your most challenging security questions • Add insight and context via brief analyst commentary to learn what FireEye knows about a threat or event • Access our experts and integrate them into your existing workflow	• Expand the capabilities of your security operations center • Get fast validation of suspected threats or alerts • Accelerate response and minimize the impact of security incidents
Fixed-Scope Services	• Invoke threat and alert investigations as needed • Request custom and finished threat intelligence from the frontlines, including digital threat assessments • Attend a spectrum of product and security training classes led by elite security practitioners • Access Intelligence Capability Development and Mandiant consulting services	• Accelerate response by investigating incidents more efficiently and effectively • Defend against emerging threats proactively with increased situational awareness • Train the way we train, using attack scenarios seen in recent breaches
Included Services	• Receive Daily News Analysis for increased situational awareness • Attend Quarterly Threat Briefings for intelligence on recent threats and trends • Includes the Mandiant Incident Response Retainer (Optional SLA available)	• Gain awareness of the latest and most important threats • Educate and raise the awareness of your entire security organization • Gain peace of mind that you are covered by Mandiant in case of an incident

Tab 9 – Required Documents

a. Clean Air and Water Act/ Debarment Notice

Clean Air and Water Act & Debarment Notice

I, the Vendor, am in compliance with all applicable standards, orders or regulations issued pursuant to the Clean Air Act of 1970, as Amended (42 U.S. C. 1857 (h), Section 508 of the Clean Water Act, as amended (33 U.S.C. 1368), Executive Order 117389 and Environmental Protection Agency Regulation, 40 CFR Part 15 as required under OMB Circular A-102, Attachment O, Paragraph 14 (1) regarding reporting violations to the grantor agency and to the United States Environment Protection Agency Assistant Administrator for the Enforcement.

I hereby further certify that my company has not been debarred, suspended or otherwise ineligible for participation in Federal Assistance programs under Executive Order 12549, "Debarment and Suspension", as described in the Federal Register and Rules and Regulations

b. Contractors Requirements

Contractor Requirements

Contractor Certification
Contractor's Employment Eligibility

By entering the contract, Contractor warrants compliance with the Federal Immigration and Nationality Act (FINA), and all other federal and state immigration laws and regulations. The Contractor further warrants that it is in compliance with the various state statues of the states it is will operate this contract in.

Participating Government Entities including School Districts may request verification of compliance from any Contractor or subcontractor performing work under this Contract. These Entities reserve the right to confirm compliance in accordance with applicable laws.

Should the Participating Entities suspect or find that the Contractor or any of its subcontractors are not in compliance, they may pursue any and all remedies allowed by law, including, but not limited to: suspension of work, termination of the Contract for default, and suspension and/or debarment of the Contractor. All costs necessary to verify compliance are the responsibility of the Contractor.

The offeror complies and maintains compliance with the appropriate statutes which requires compliance with federal immigration laws by State employers, State contractors and State subcontractors in accordance with the E-Verify Employee Eligibility Verification Program.

Contractor shall comply with governing board policy of the NCPA Participating entities in which work is being performed

Fingerprint & Background Checks

If required to provide services on school district property at least five (5) times during a month, contractor shall submit a full set of fingerprints to the school district if requested of each person or employee who may provide such service. Alternately, the school district may fingerprint those persons or employees. An exception to this requirement may be made as authorized in Governing Board policy. The district shall conduct a fingerprint check in accordance with the appropriate state and federal laws of all contractors, subcontractors or vendors and their employees for which fingerprints are submitted to the district. Contractor, subcontractors, vendors and their employees shall not provide services on school district properties until authorized by the District.

The offeror shall comply with fingerprinting requirements in accordance with appropriate statutes in the state in which the work is being performed unless otherwise exempted.

Contractor shall comply with governing board policy in the school district or Participating Entity in which work is being performed

Business Operations in Sudan, Iran

In accordance with A.R.S. 35-391 and A.R.S. 35-393, the Contractor hereby certifies that the contractor does not have scrutinized business operations in Sudan and/or Iran.

[redacted]

c. *Antitrust Certification Statements*

Antitrust Certification Statements (Tex. Government Code § 2155.005)

I affirm under penalty of perjury of the laws of the State of Texas that:

(1) I am duly authorized to execute this contract on my own behalf or on behalf of the company, corporation, firm, partnership or individual (Company) listed below;

(2) In connection with this bid, neither I nor any representative of the Company has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15;

(3) In connection with this bid, neither I nor any representative of the Company has violated any federal antitrust law; and

(4) Neither I nor any representative of the Company has directly or indirectly communicated any of the contents of this bid to a competitor of the Company or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Company.

Company name Global Solutions Group, Inc.

Address 25900 Greenfield Road, Suite 220

City/State/Zip Oak Park, MI 48237

[redacted]

d. Required Clauses for Federal Funds Certifications

GSG acknowledges and agrees with all the clauses for federal funds certification provided in the RFP.

e. Required Clauses for Federal Assistance by FTA

GSG acknowledges and agrees with all the clauses for federal assistance by FTA provided in the RFP.

f. State Notice Addendum

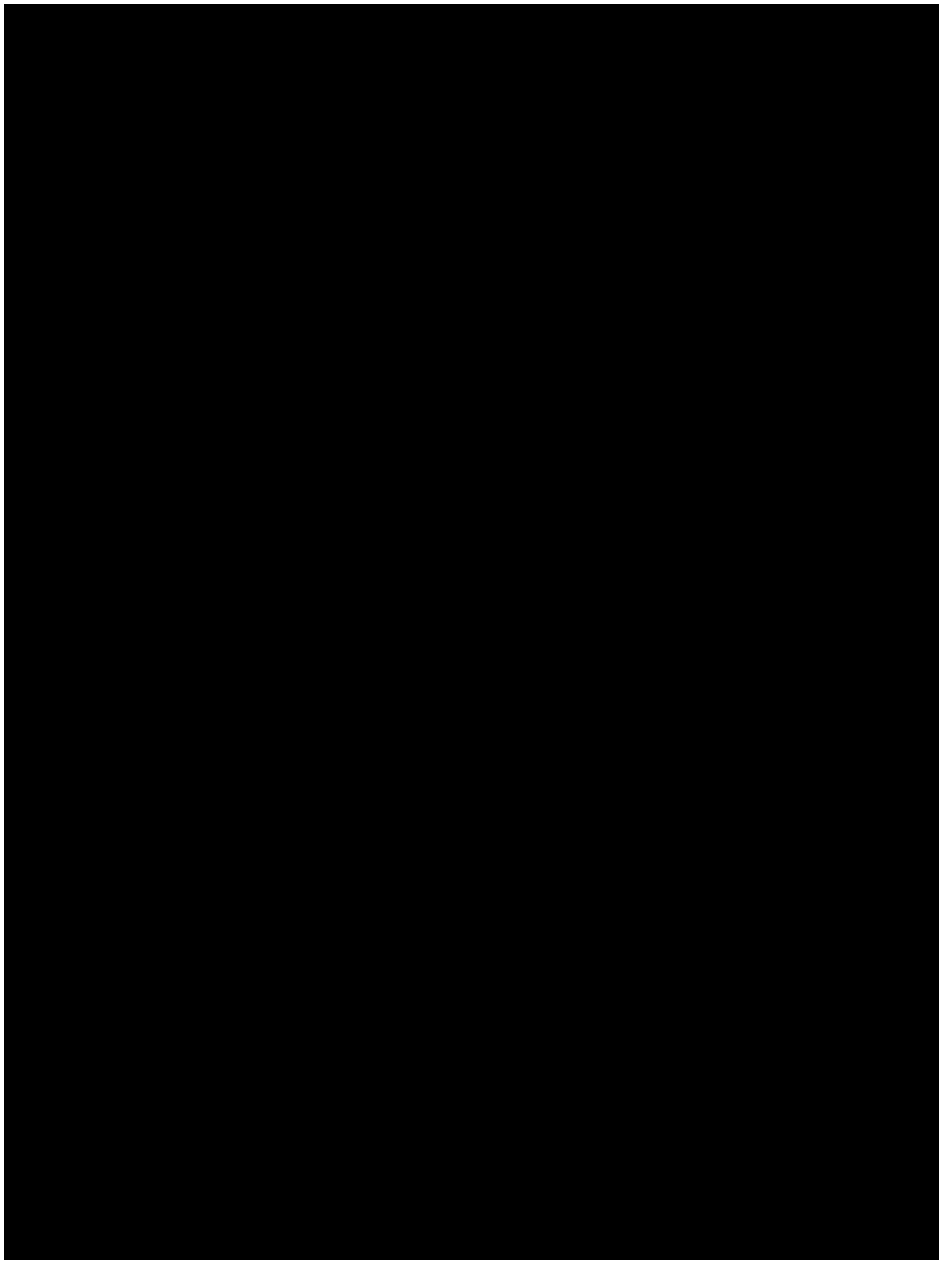
As of November 18, 2021, no addenda have been posted.

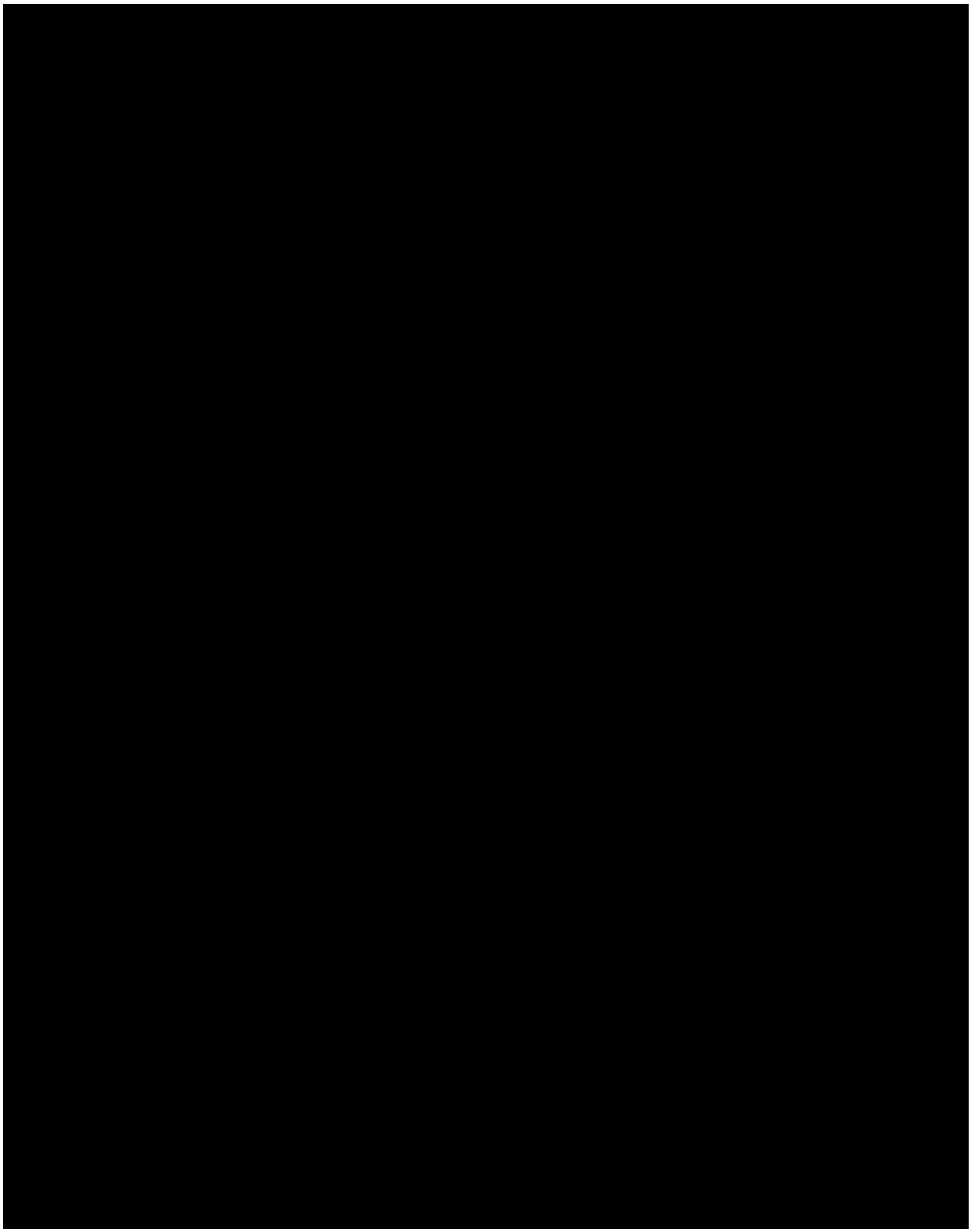
Appendix I – Performance Reviews

The following are Contract Performance Assessment Reporting System (CPARS) evaluations for several Cybersecurity engagements. These are official assessments of performance made by federal government agencies regarding contractor performance on contracts. As you can see, GSG's clients are exceptionally satisfied.

The following are Contractor Performance Assessment Reports (CPARS), which are official reviews of contractor performance from federal government agencies.

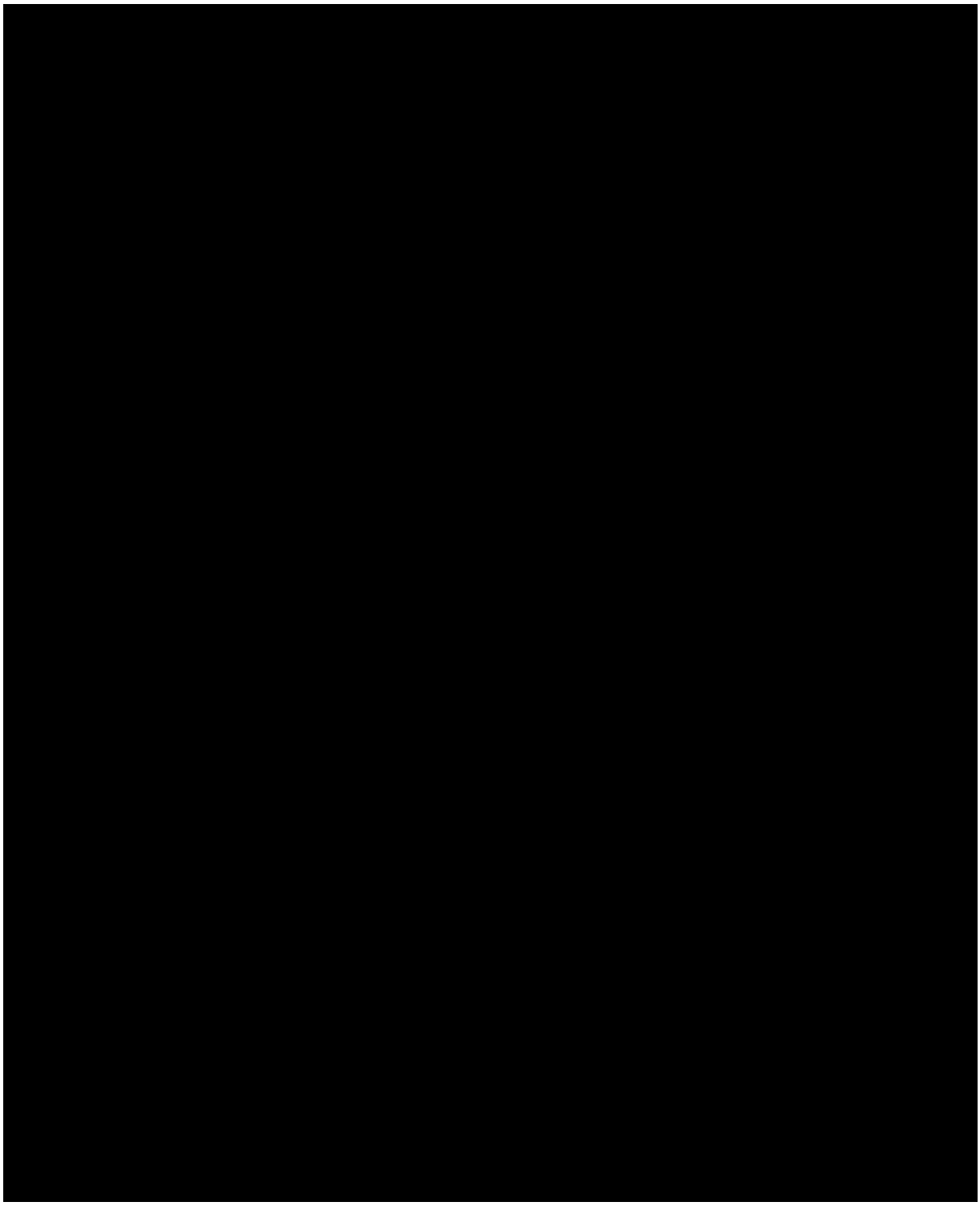
Web Application Assessment of [redacted]





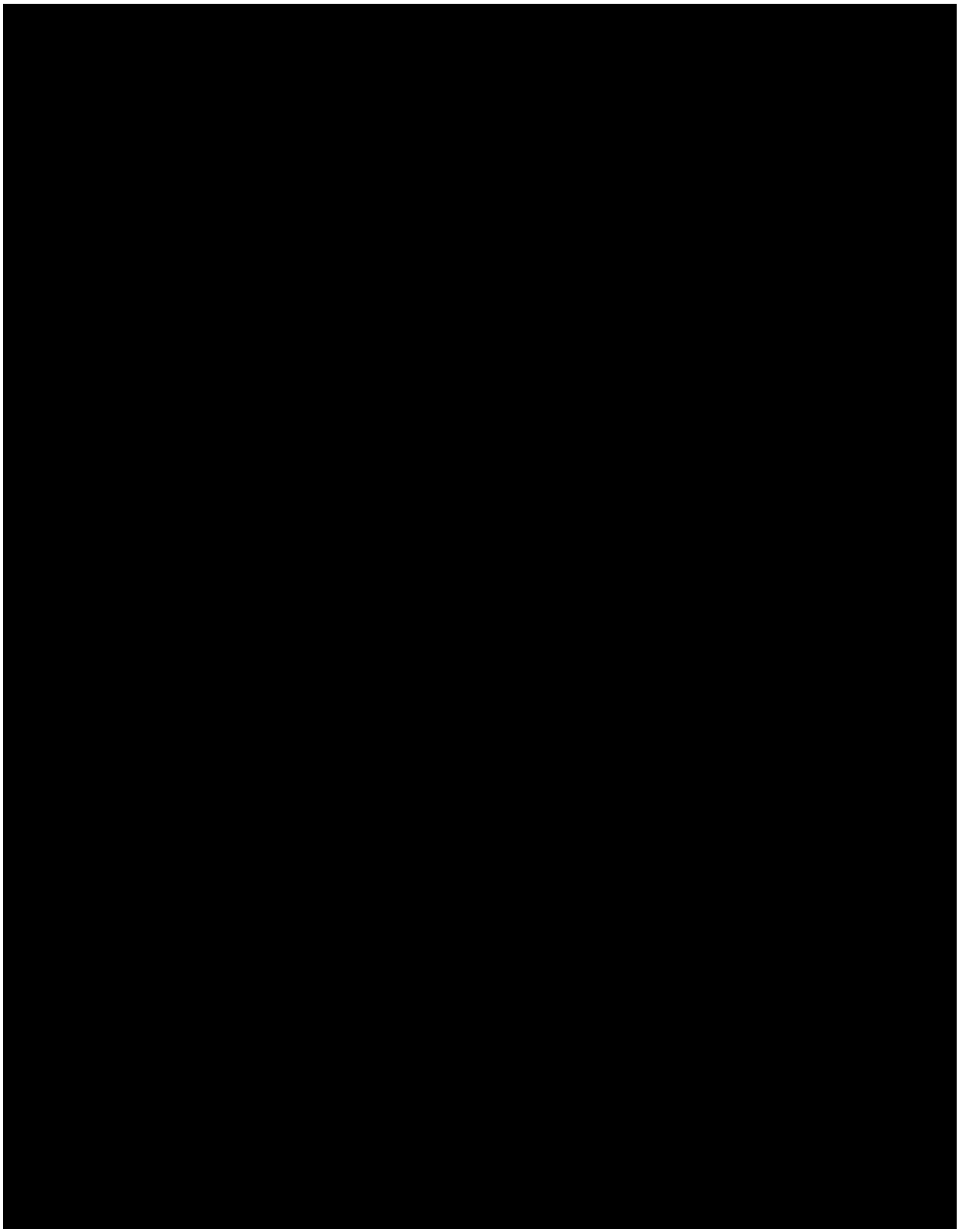
Operational Security Assessments for [redacted]

[redacted]



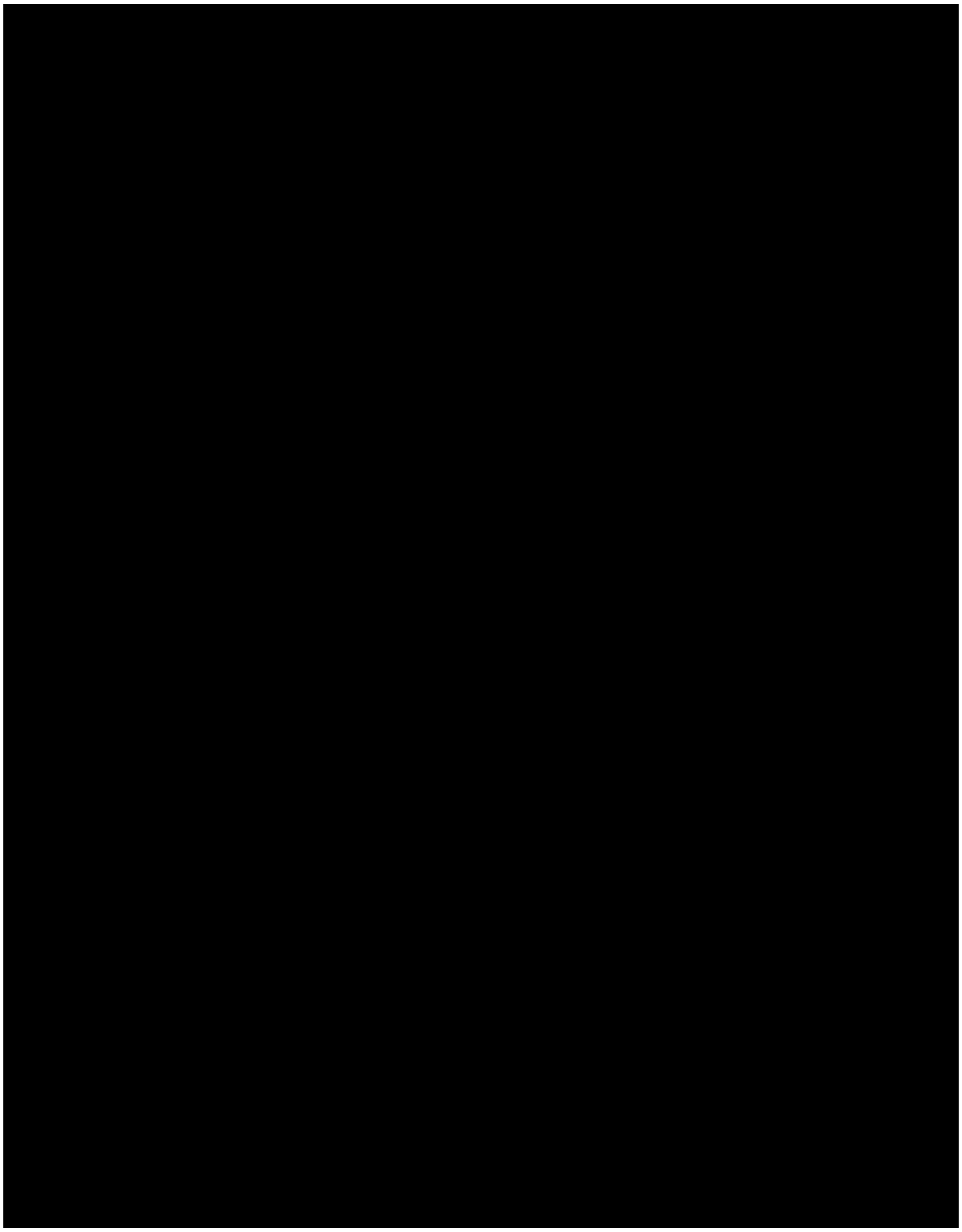
Penetration Test of [redacted]

[redacted]



Penetration Test of [redacted]

[redacted]



The following is a description of the Penetration Test of [redacted] 2017–2018 project for which we received the above evaluation (with the exception of the schedule, it also describes the activities for penetration test of [redacted] during the contract period) which demonstrates our capability to perform complex cybersecurity services over a dispersed geographic area — including vulnerability assessment and penetration testing projects:

Penetration Test of Multiple USDA Agencies	
Client	[redacted]
Role of the Firm	GSG provided a Penetration Test Team to perform penetration testing of the agency's systems, network, and IT environment under the USDA Rules of Engagement. Our Penetration Test Team performed the penetration tests designed to detect network and system vulnerabilities. A Red Teaming engagement was executed in testing security by taking an attacker-like approach to system/network/data access. A Red Teaming approach is in-depth and comprehensive and aims at finding all possible vulnerabilities for a given system, network, and IT environment in order to assess the associated risk. The Red Teaming approach tested for all types of attacks (access, modification, denial of service, and repudiation) to provide a complete penetration test/security assessment report. The Penetration Testing Team performed the penetration test as follows: 1. Probed each host's Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports using a port scanner to determine what network services were being provided by each host. 2. Scanned each host's available network services for known, remotely exploitable vulnerabilities. 3. When access to a host was possible, the OSAT Penetration Testing Team connected to the affected system and probed for known locally exploitable vulnerabilities. The three primary objectives of this step were to: • Obtain administrator privileges • Perform privilege escalation (domain administrator rights) • Move laterally throughout the network
Outcome	• Identified existing system-specific and architectural vulnerabilities and recommended countermeasures to mitigate the risks to system confidentiality, integrity, and availability. • Provided the 'footprint' of the tested networks — the hosts/services available to potential attackers. This allowed the agencies to better manage risk and make appropriate preventative decisions as technology and attack methods evolve.

Project Schedule

Initial Project Schedule

September 30, 2017, through September 29, 2018

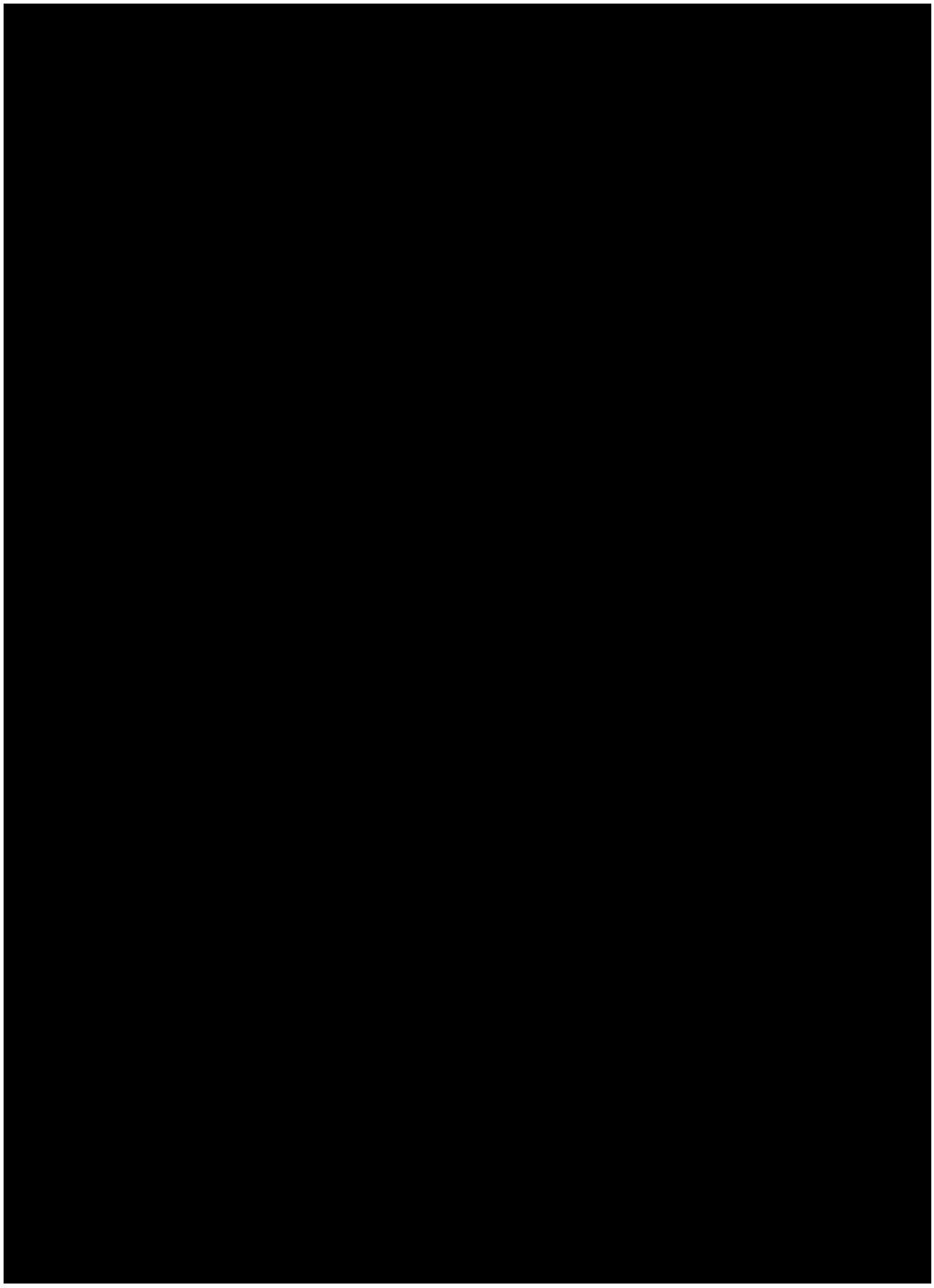
Agency	Start Date	End Date
[redacted]	10/1/2017	10/30/2017
[redacted]	11/1/2017	11/30/2017
[redacted]	11/27/2017	12/27/2017
[redacted]	12/1/2017	12/30/2017
[redacted]	11/1/2017	11/30/2017
[redacted]	12/1/2017	12/30/2017
[redacted]	12/1/2017	1/31/2018
[redacted]	1/1/2018	1/31/2017
[redacted]	2/1/2018	3/31/2017
[redacted]	2/1/2018	3/31/2018
[redacted]	4/1/2018	6/30/2018
[redacted]	4/1/2018	6/30/2018
[redacted]	4/1/2018	6/30/2018
[redacted]	4/1/2018	6/30/2018
[redacted]	4/1/2018	6/30/2018
[redacted]	4/1/2018	6/30/2018
[redacted]	7/1/2018	8/31/2018
[redacted]	7/1/2018	8/31/2018
NIFA	9/1/2018	9/3/2018
Post-assessment/Final Report		9/29/2018

Final Project Schedule Additions

The following additions to the schedule extended the completion date through November 31, 2018:

[redacted]	9/10/2018	9/15/2018
[redacted]	9/24/2018	9/27/2018
Post-assessment/Final Report		11/31/2018

The following is a performance review from the [redacted]:

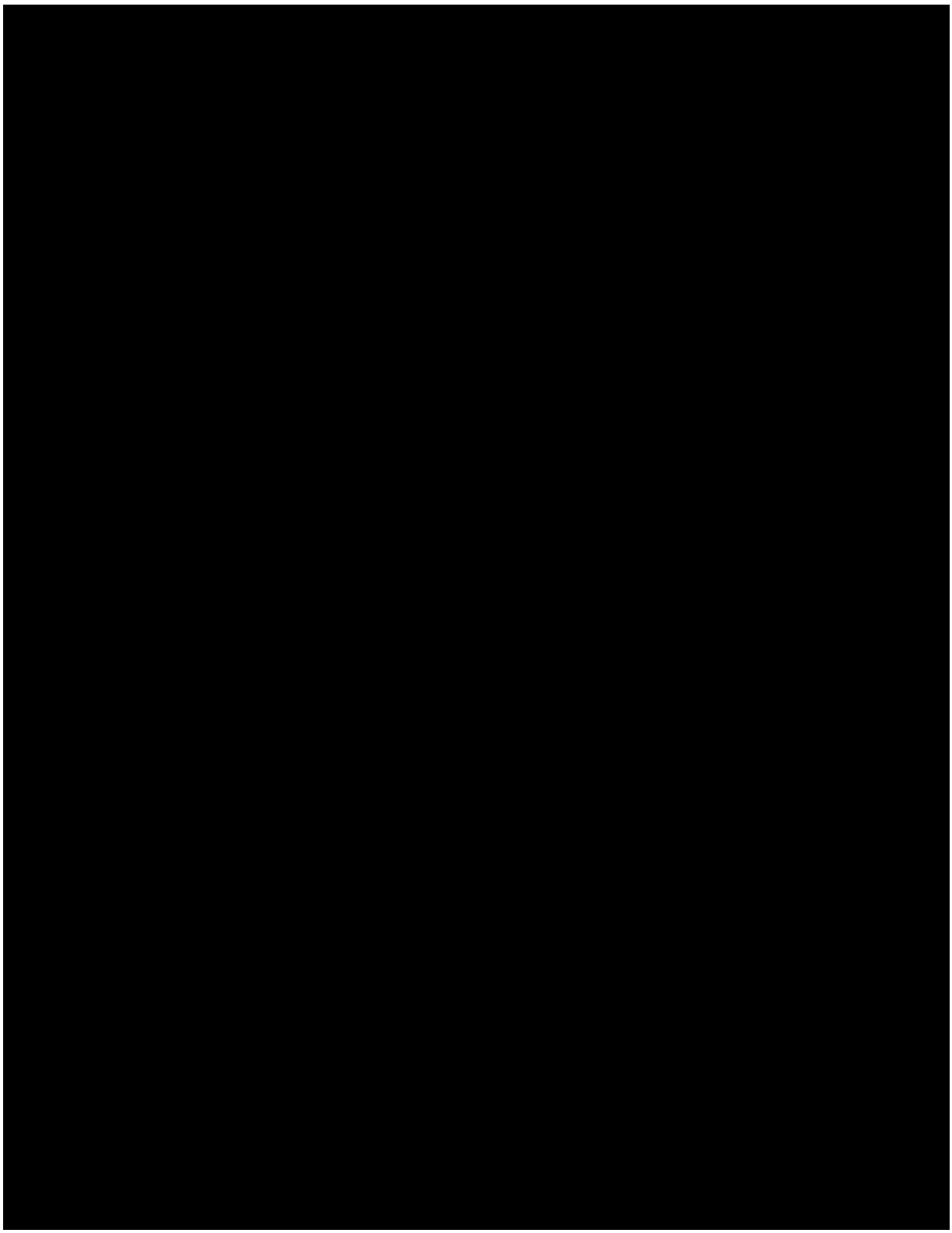


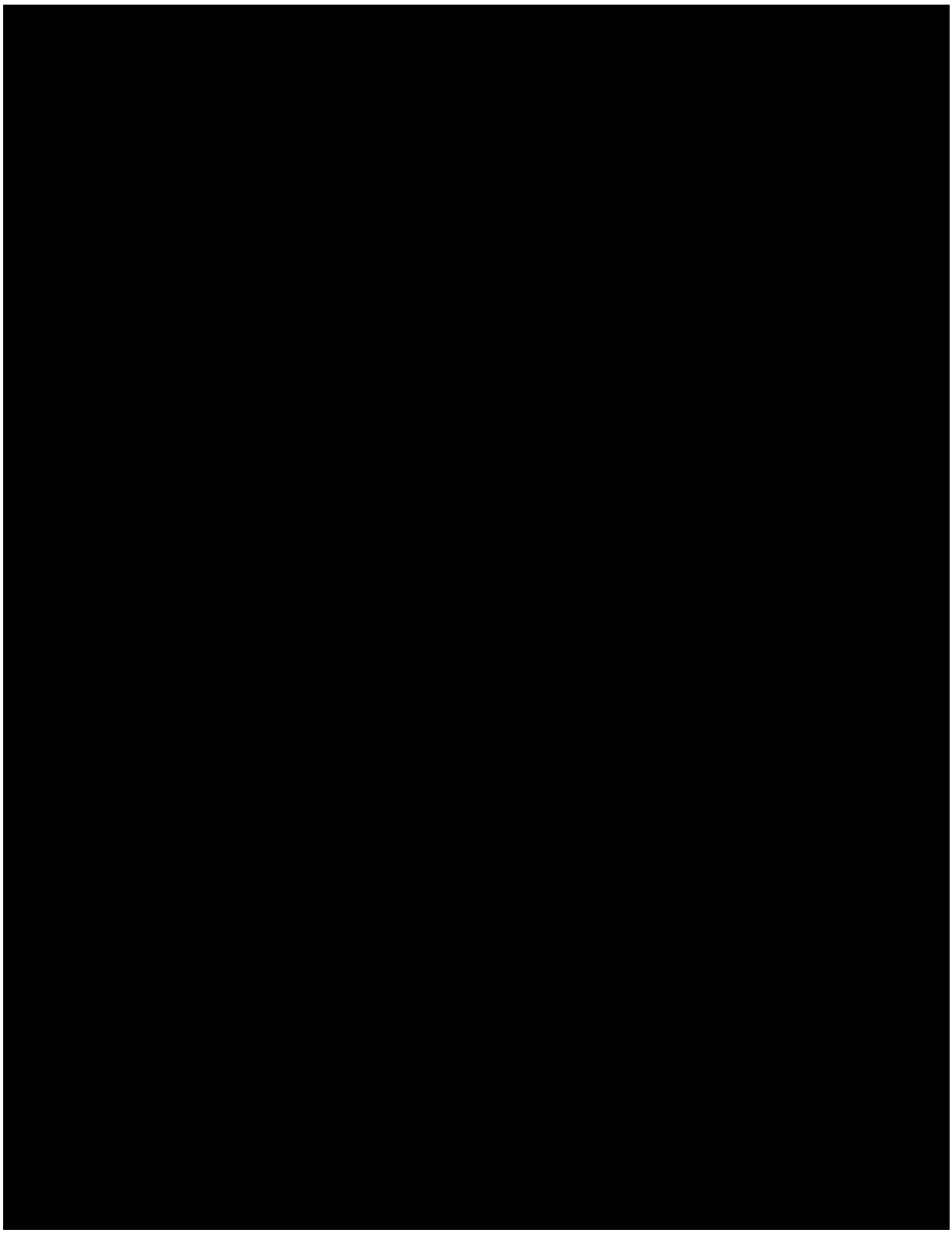
The following is a performance review from the [redacted]

[redacted]

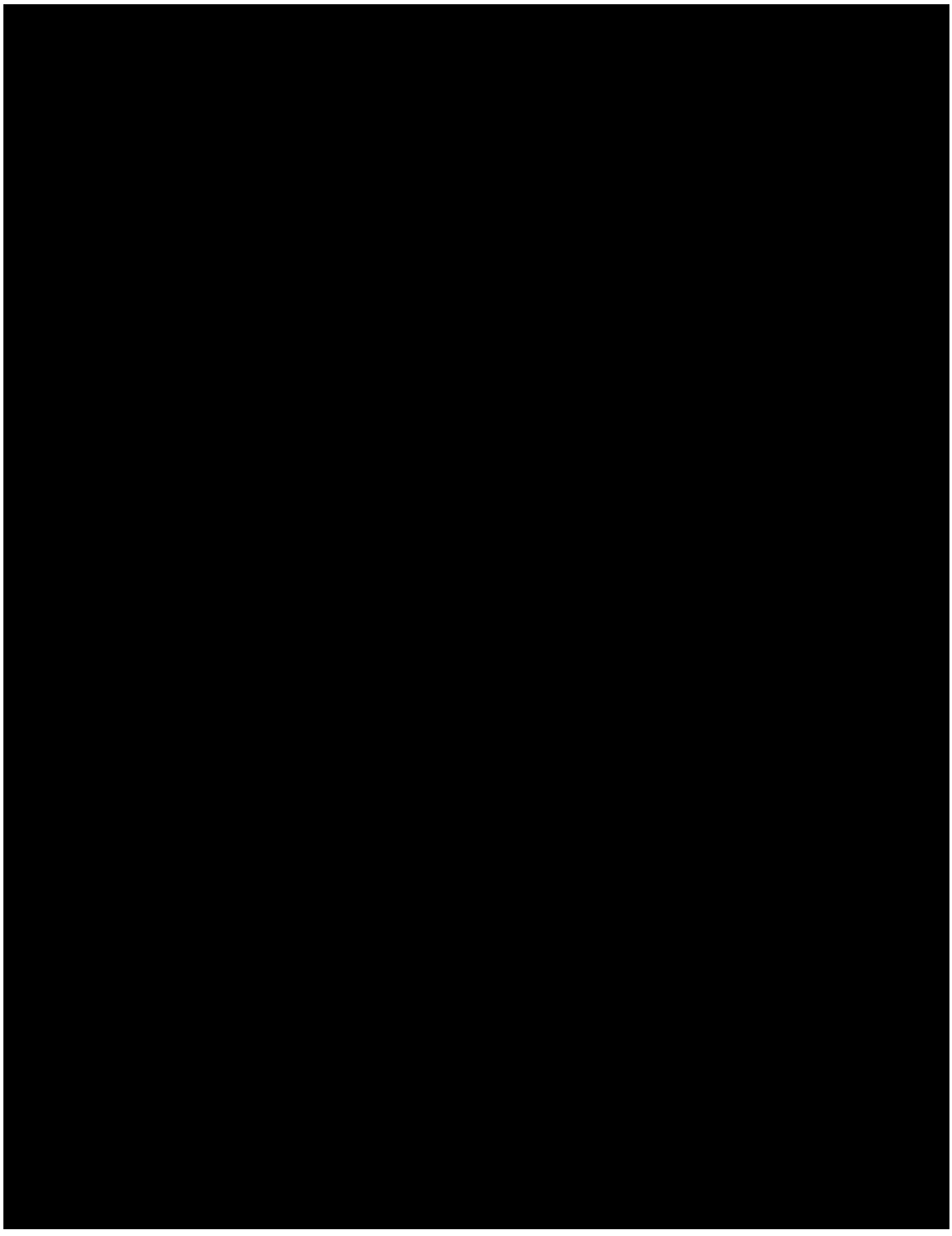
Information Security Center – Security Assessment Team, Penetration Testing – Exit Survey Questionnaire for [redacted]

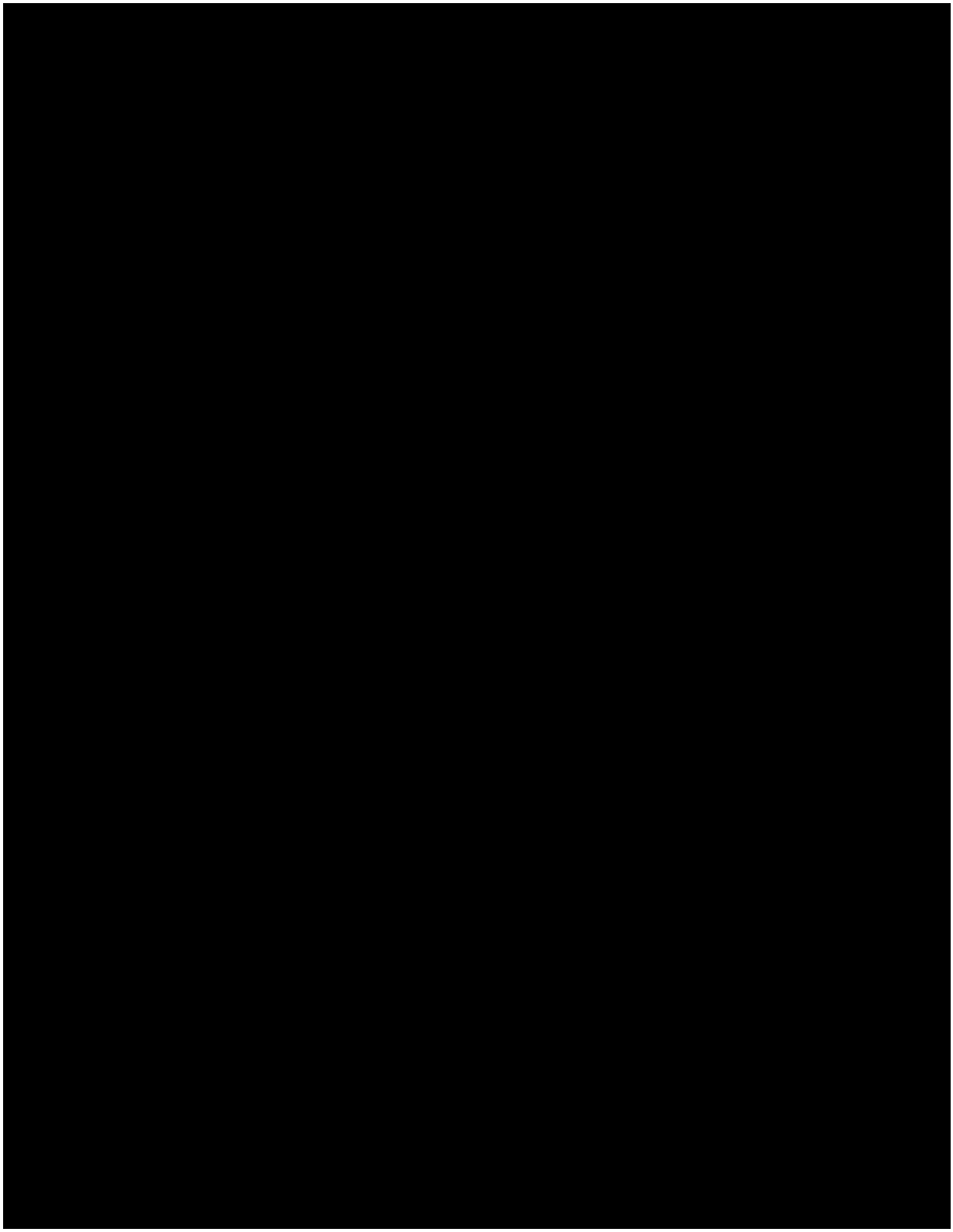
[redacted]

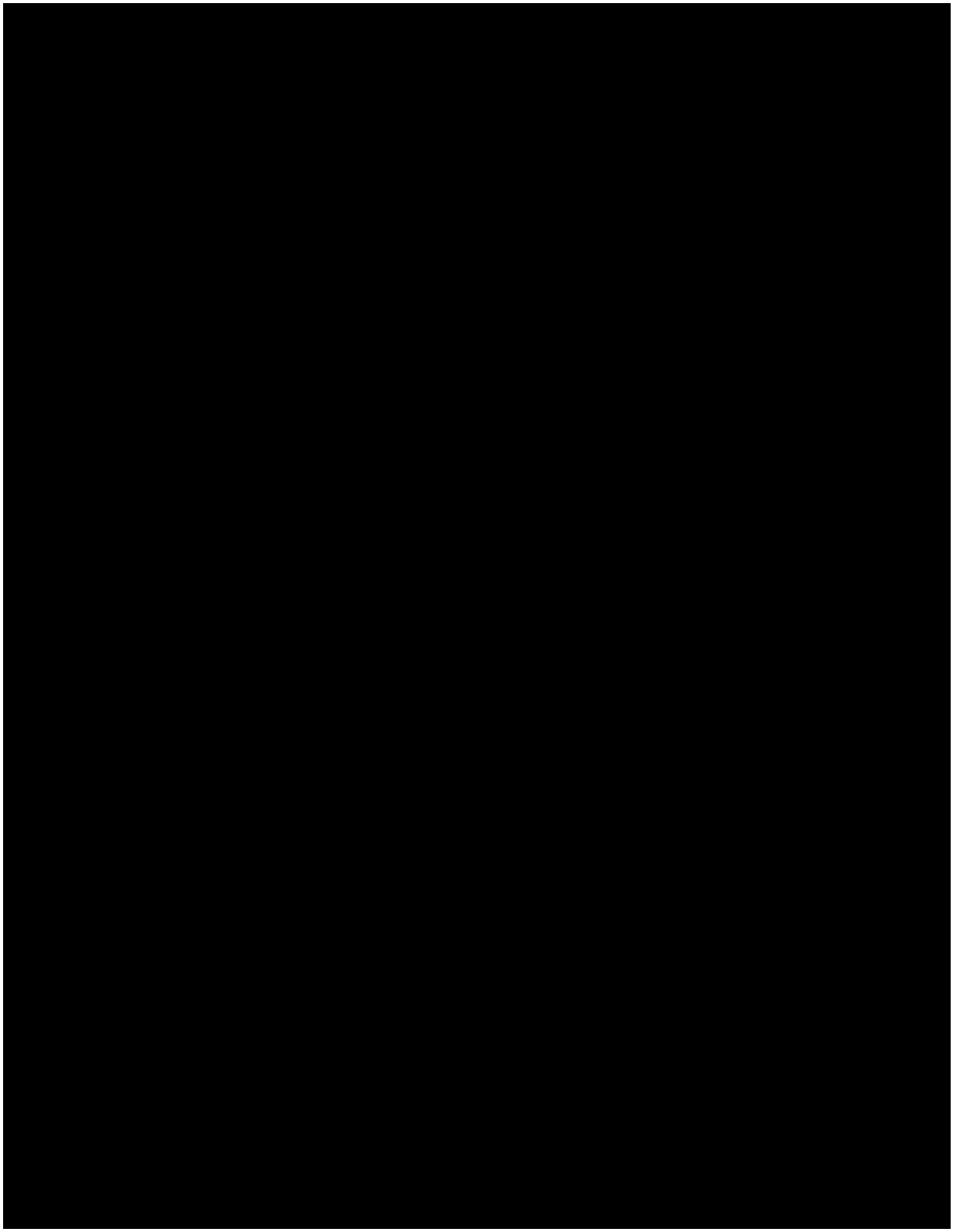


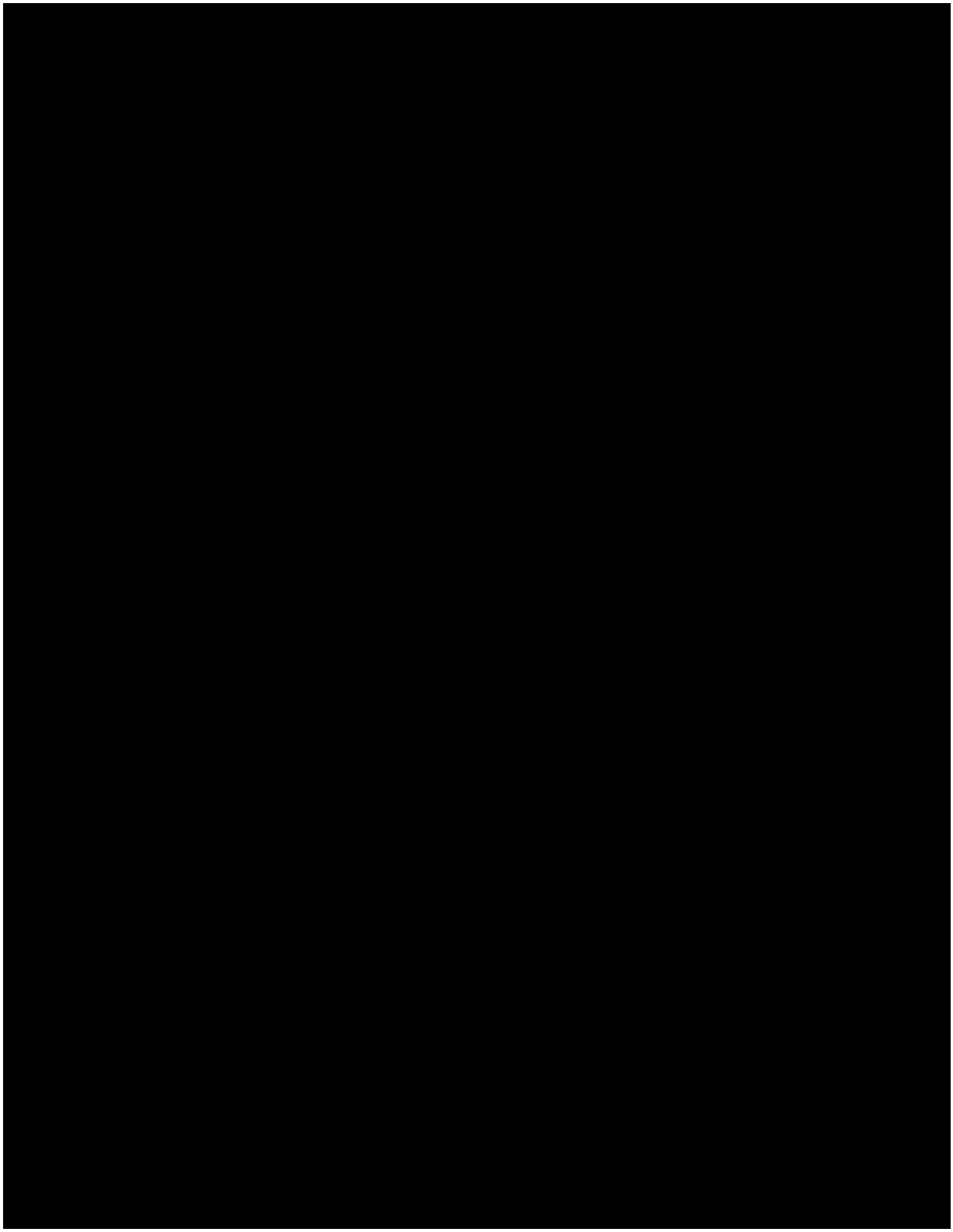


Information Security Center – Security Assessment Team, Penetration Testing – Exit Survey Questionnaire for [redacted]

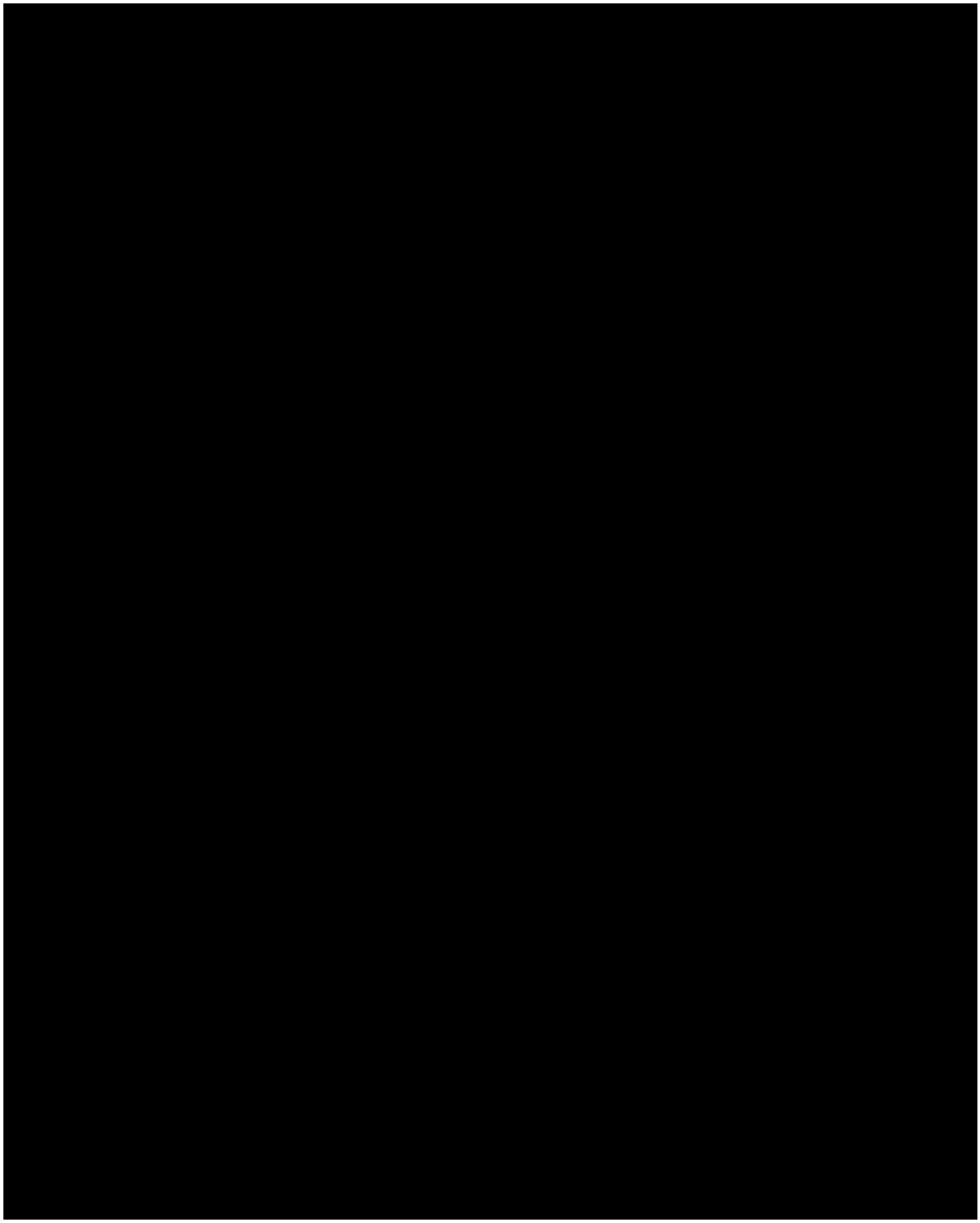


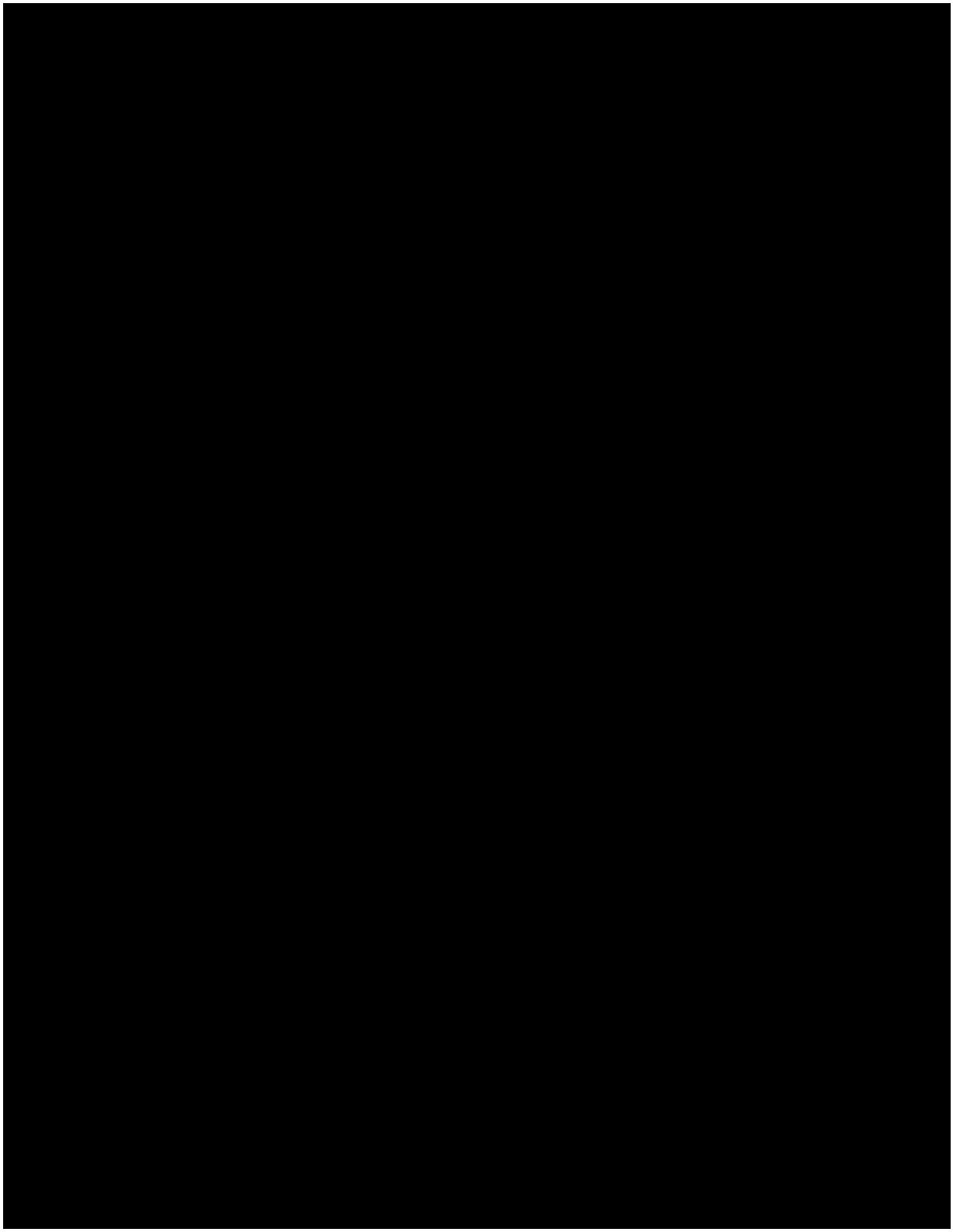


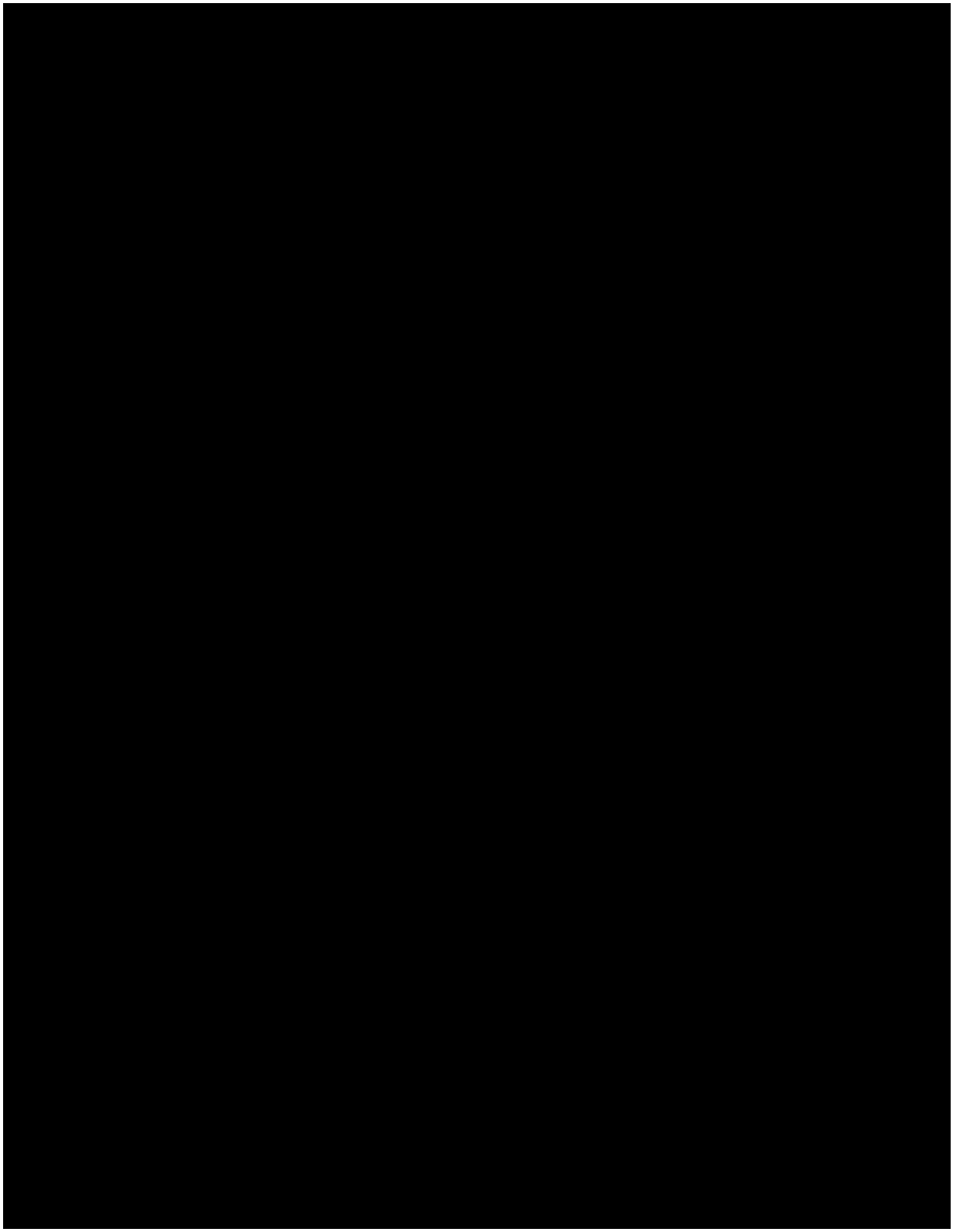


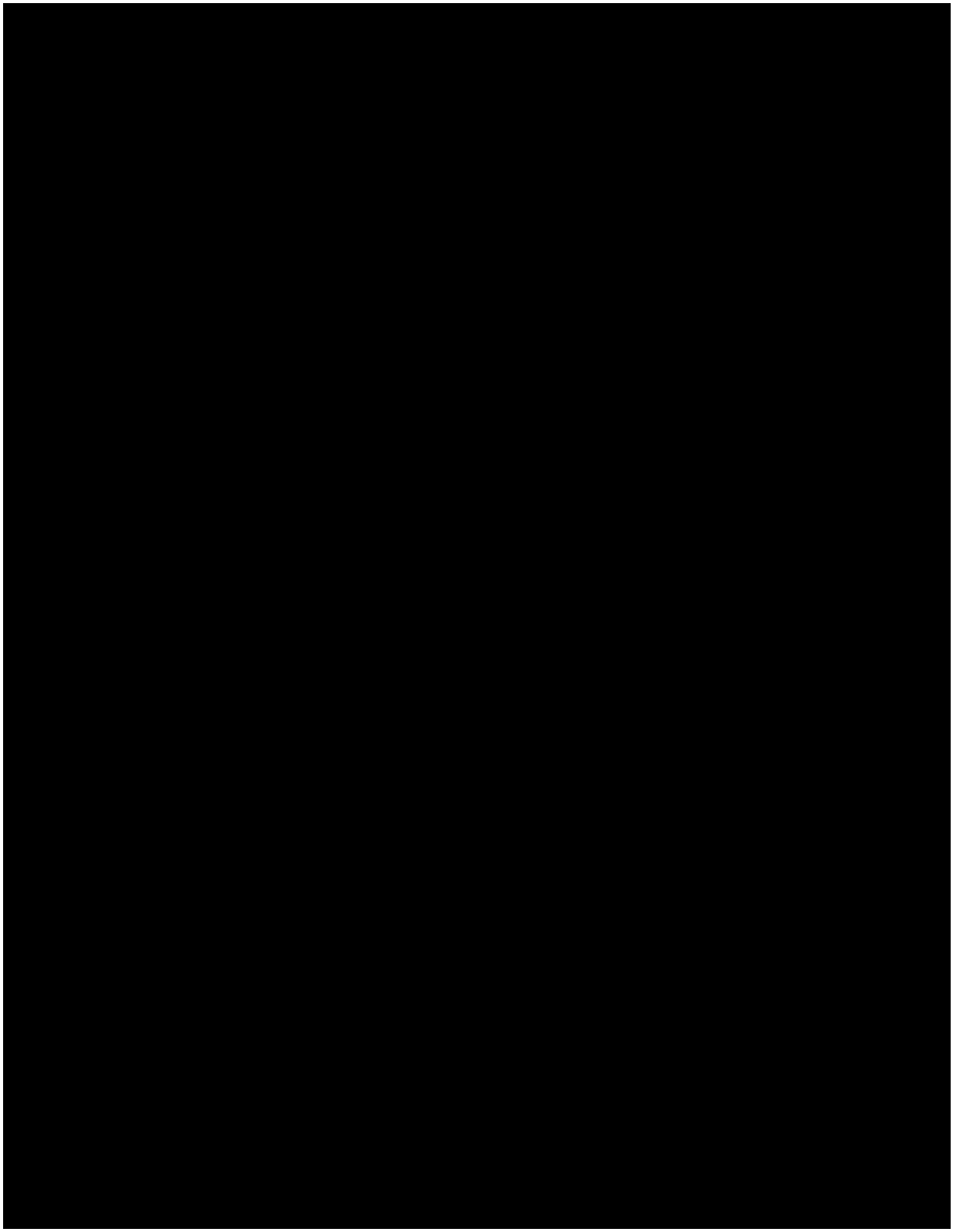


Information Security Center – Security Assessment Team, Penetration Testing – Exit Survey Questionnaire for Agriculture Marketing Services









CERTIFIED RESELLER

amazon web services

ORACLE PARTNERNETWORK

Laserfiche®
Authorized Reseller

IBM PartnerWorld

Canon

Microsoft Gold Partner

FIREEYE

FORTINET
AUTHORIZED PARTNER