

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION**

NETWORK INTEGRITY SYSTEMS, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No.: <u>3:25cv268</u>
	)	
CYBERSECURE IPS LLC,	)	JURY TRIAL DEMANDED
	)	
Defendant.	)	
	)	

COMPLAINT

Plaintiff Network Integrity Systems, Inc. (“NIS”), by and through its undersigned counsel, complains of Defendant CyberSecure IPS LLC (“CS”), and alleges as follows:

NATURE OF THE SUIT

1. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code, involving infringement of U.S. Patent No. 7,706,641 (“the ‘641 patent” or “patent-in-suit”, attached as **Exhibit 1**, in reference to the patent claim chart, attached as **Exhibit 2**, incorporated herein by reference).

PARTIES, JURISDICTION AND VENUE

2. NIS is a North Carolina corporation with a principal place of business at 1937 Tate Boulevard SE, Hickory, North Carolina 28602.

3. CS is a Maryland limited liability company headquartered in Herndon, Virginia.¹

4. This Court has jurisdiction over this matter pursuant to 28 U.S.C. §§ 1331 and

¹ <https://www.linkedin.com/company/cybersecure-ips/about/>.

1338(a).

5. Personal jurisdiction exists over CS because it has its headquarters in Virginia where it also conducts regular business and engaged in infringement.

6. Venue is proper under 28 U.S.C. § 1400(b) in this Division and District where CS has committed acts of infringement and has a regular and established place of business.

FACTUAL BACKGROUND

7. NIS owns patents in the field of optical fiber security and is a cyber-security business and leading provider of optical sensing technology for cyber and physical security applications specializing in optical fiber monitoring to enhance network infrastructure security across various sectors.

8. CS is also a cyber-security business that specializes in the design and development of prepackaged computer software and fiber-optic-based solutions for network infrastructure security.

9. The parties have a long history of working together. Effective October 1, 2015, the parties entered into an Exclusive Strategic Relationship Agreement (“ESR Agreement”) related to integration and joint sale of technology solutions to customers.

10. Effective June 23, 2023, the parties terminated the ESR Agreement and entered into a Memorandum of Understanding (“MOU”) to continue working together to service customers after the termination of the ESR Agreement. This Complaint is limited to CS’s infringing activity after the termination of the ESR Agreement on June 23, 2023.

11. Effective September 5, 2024, the parties entered into a “Settlement Agreement” (the “Settlement Agreement”) whereby they resolved various MOU disputes, including claims by NIS that CS improperly hired current and former NIS employees who were subject to non-

competition and/or non-solicitation clauses in their employment contracts with NIS, and that CS disclosed and/or misused confidential NIS information.

12. The '641 patent is entitled "MONITORING INDIVIDUAL FIBERS OF AN OPTICAL CABLE FOR INTRUSION" and was duly and legally issued by the United States Patent and Trademark Office on April 27, 2010.

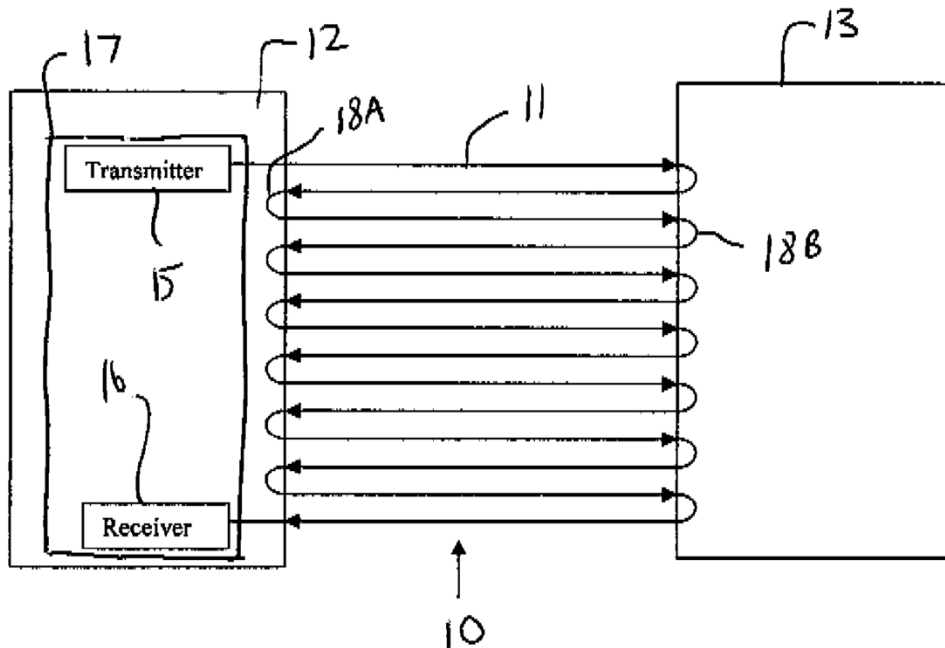
13. The '641 patent includes method claims related to detecting movement of optical fibers of an optical fiber cable and generating an alarm indicating the movement.

14. The '641 patent is valid and enforceable.

15. NIS is the exclusive owner of all right, title, and interest in the '641 patent. NIS practices the technology disclosed in the patents and has the right to bring this action to recover damages for any current or past infringement of these patents. CS does not have a license to practice the inventions claimed in the '641 patent.

16. The '641 patent is directed to a system and method for detecting movement of optical fibers for the purpose of intrusion detection. The claims of the '641 patent are method claims that include method steps such as injecting light into fibers to be monitored and receiving light signals that have been transmitted along the fibers being monitored. At least claims 1 and 12 of the '641 patent read on a point-to-multipoint network layout where the number of fibers being monitored is greater than the number of light sources and greater than the number of sensor arrangements that detect the light being transmitted through the monitored fibers.

17. Fig. 1 of the '641 patent (set forth below) depicts an exemplary point-to-multipoint network layout.



18. NIS manufactures and sells two products that are relevant to the '641 patent. The "Interceptor" and "Vanguard," which are both interrogator type devices that provide light to optical fibers being monitored and receive light signals from those fibers. The received light signals are analyzed for abnormalities that indicate whether there is an intrusion into the cable carrying the fiber or the fiber itself. The analysis of the light signals may be performed by software in the interrogator device or by software on a separate computer providing a user interface, or both. Both the Interceptor and Vanguard devices are capable of protecting up to 8-separate zones or cable paths distributed throughout the building by monitoring strands of fibers within optical cables making up the network infrastructure.

19. A system operating with a NIS Interceptor or Vanguard device detects and reports tampering or intrusion attempts for the purposes of data theft (tapping) or denial of service attacks. The Interceptor and Vanguard devices are designed to be used in a detection system and method that utilizes a point-to-multipoint network layout.

20. On information or belief, CS has had knowledge of the ‘641 patent at least since the parties entered into the ESR Agreement in 2015. CS personnel have frequently visited NIS facilities where a plaque showing the cover page of the ‘641 patent is displayed. In addition, CS personnel attended training at NIS facilities where the NIS innovations (*e.g.*, network intrusion monitoring using point-to-multipoint network layout) covered by the ‘641 patent were described as “patented.” NIS and CS created and distributed co-branded marketing materials that referenced NIS’ “patented hub and spoke technology.” Two examples of these marketing materials are attached as **Exhibit 3**. In addition, on information and belief, CS conducted a review of NIS’s patent portfolio (including the ‘641 patent) in 2023 when the ESR Agreement was terminated.

21. Until the parties severed their relationship in 2024, CS partnered with NIS to offer both CS and NIS products to their joint customers. These joint customers included both data center customers who purchased and installed numerous Vanguard devices and practiced the claims of the ‘641 patent, and customers who operated Protective Distribution Systems (PDS) and purchased and installed numerous Interceptor devices. One of the parties’ data center customers (the “Primary Customer”) was responsible for the vast majority of the parties’ data center related business.

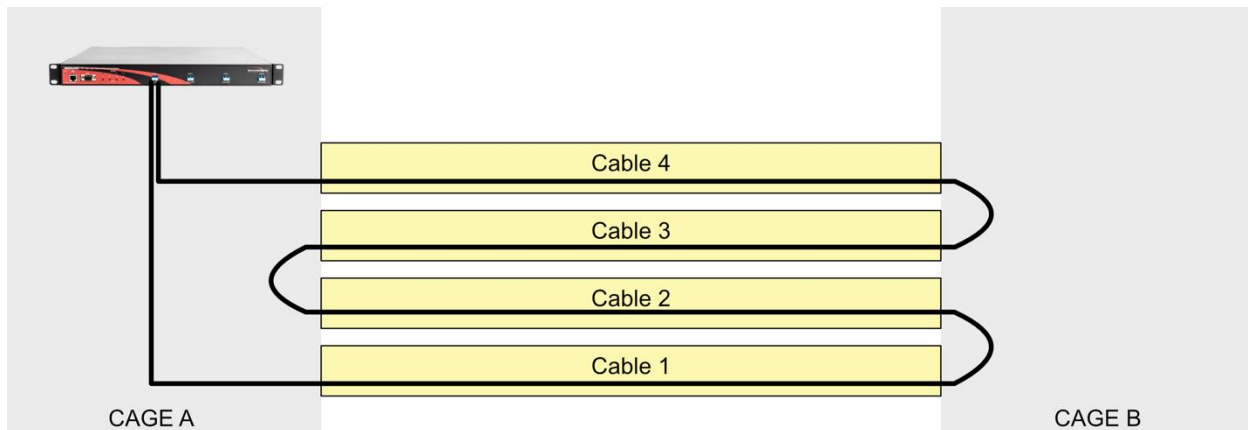
22. During the approximately nine years that the parties co-marketed products, CS did not have a product that competed with the NIS Interceptor and Vanguard devices. CS is now offering for sale and selling a product that competes with the NIS Interceptor and Vanguard devices. CS has incorporated the functionality of the Interceptor and Vanguard devices into a newly marketed device named “Opti-Guard.” CS marketing materials for the Opti-Guard device are attached as **Exhibits 4** and **5**. CS touts its Opti-Guard device to customers as a device that can “replace the [NIS] Interceptor.” Ex. 5 at p. 2.

23. As described further below, CS makes, uses, sells, and/or offers for sale products and services that infringe the ‘641 patent. These products and services include intrusion systems and methods that include both software and hardware devices. In particular, CS makes, uses, sells, and/or offers for sale at least the following products and services that infringe the ‘641 patent (“Accused Products and Services”):

- a. Detection System and Method used in Data Centers;
- b. Detection System and Method used in Protected Distribution Systems (PDS); and
- c. Detection System and Method used in Manhole, Lockbox, and other Fiber Bragg Grating (FBG) Intrusion Monitoring.

CyberSecure’s Infringing Detection System and Method used in Data Centers

24. Until its relationship with NIS ended in 2024, CS partnered with NIS to pair its software with the NIS Vanguard device for use in data centers for monitoring movement of optical fibers. CS now offers an alternative to the NIS Vanguard device, and offers for sale, sells, and has sold its software and hardware for use in a system and method for monitoring intrusion of OSP/ISP Pathways and Conduits for various data centers having a point-to-multipoint network layout. An exemplary layout of a commercial point-to-multipoint network layout is set forth below:



25. Use of these CS products in a system and method for monitoring intrusion of OSP/ISP Pathways and Conduits for use in an intrusion detection system with a point-to-multipoint network layout infringes at least claims 1 and 12 of the '641 patent, either literally or under the doctrine of equivalents, because such a detection system including CS products performs all of the steps required in these claims, as set forth in detail in Exhibit 2.

26. In particular, CS has offered for sale and sold its products for use in a system and method for monitoring intrusion of OSP/ISP Pathways and Conduits for use in data centers owned by the Primary Customer that employ an intrusion detection system with point-to-multipoint network layout. The CS products and services for sale and sold for use in data centers are described on the CS website. ("Realize True Data Center Security with CyberSecure IPS", attached as **Exhibit 6.**)

27. For certain Primary Customer data centers, CS has offered for sale and sold its products to replace existing NIS Vanguard device already in use in the point-to-multipoint network layouts in the Primary Customer data centers. In particular, NIS began providing its Vanguard devices to the Primary Customer in 2017 for use in data centers that include a point-to-multipoint network layout and are located in this Division and District. The Primary Customer has a life cycle replacement policy that requires it to replace electronic devices at least every seven years. CS has offered for sale and sold its OptiGuard device to replace Vanguard devices located in this Division and District, in response to the Primary Customer acting according to its life cycle replacement policy. The CS system and method that includes the OptiGuard and is being offered for sale and sold for use in the Primary Customer data centers with a point-to-multipoint network layout infringes at least claims 1 and 12 of the '641 patent.

28. CS, with knowledge of the '641 patent and knowledge that the CS intrusion detection system and method used in the point-to-multipoint network layout at Primary Customer data centers infringes the '641 patent, provides assistance and instruction in connection with the installation and use of the CS intrusion detection system at the Primary Customer data centers and the knowhow to use the CS intrusion detection system in an infringing manner.

29. CS, with knowledge of the '641 patent and knowledge that the CS intrusion detection system and method used in the point-to-multipoint network layout at Primary Customer data centers infringes the '641 patent, directs its salespeople and technical personnel to conduct troubleshooting and testing on the CS intrusion detection system used in the point-to-multipoint network layout at Primary Customer data centers.

30. The infringing CS intrusion detection system and method is designed for use with the point-to-multipoint network layout at Primary Customer data centers in a manner that infringes the '641 patent.

CyberSecure's Infringing Detection System and Method used in Protected Distribution Systems (PDS)

31. Until its relationship with NIS ended in 2024, CS partnered with NIS to pair its software with the NIS Interceptor device for use with a PDS for monitoring movement of optical fibers. CS now offers an alternative to the NIS Interceptor device – the Opti-Guard device -- and offers for sale, sells, and has sold its own products for use in a system and method for monitoring intrusion of optical fibers in a PDS.

32. The CS products and services for sale for use with a PDS are described on the CS website. ("Alarmed Carrier PDS Solutions For Military and Government," attached as **Exhibit 7**.) CS has offered for sale and sold its products for use in a system and method for monitoring intrusion of the PDS used in a secure government facility located in the District of Columbia,

Maryland and Virginia region (the “DMV Facility”).

33. The DMV Facility is well known to CS because CS knew it was competing with NIS to provide products and services to monitor PDS intrusion at the DMV Facility. CS and NIS were working with the same integration company that was offering CS and NIS products as alternative solutions to the DMV Facility. The cables used at the DMV Facility include air blown optical fibers which, although not unique, distinguish the DMV Facility from other government facilities that employ a PDS. The CS products and services offered for sale and sold for use at the DMV Facility include an intrusion detection system for a PDS with a point-to-multipoint network layout. Use of the CS products in a system and method for monitoring intrusion of the PDS used at the DMV Facility infringes at least claims 1 and 12 of the ‘641 patent, either literally or under the doctrine of equivalents, because such an intrusion detection system including CS products performs all the steps required in these claims, as set forth in detail in Exhibit 2.

34. CS, with knowledge of the ‘641 patent and knowledge that the CS intrusion detection system used in the PDS with a point-to-multipoint network layout at the DMV Facility infringes the ‘641 patent, provides assistance and instruction in connection with the installation and use of the CS intrusion detection system at the DMV Facility and the knowhow to use the CS intrusion detection system in an infringing manner.

35. CS, with knowledge of the ‘641 patent and knowledge that the CS intrusion detection system used in the PDS with a point-to-multipoint network layout at DMV Facility infringes the ‘641 patent, directs its salespeople and technical personnel to conduct troubleshooting and testing on the CS intrusion detection system used at the DMV Facility.

36. When deployed for use with the PDS with a point-to-multipoint network layout at the DMV Facility, the CS intrusion detection system and method is specifically designed in a manner that infringes the ‘641 patent.

CyberSecure’s Infringing Detection System and Method used in Manhole, Lockbox, and other Fiber Bragg Grating (FBG) Intrusion Monitoring

37. In addition to those infringing detection systems and methods discussed above that are used with networks arranged in a point-to-multipoint layout, CS also manufactures, distributes, offers to sell and sells its “Controller,” “Opti-Guard,” and “Cyber Sensor” products (<https://www.cybersecureips.com/our-products/>) for use in a system and method for monitoring intrusion of manholes, lockboxes, and other purposes.

38. Use of the CS Controller, Opti-Guard, and/or Cyber Sensor Products for manhole, lockbox, and other FBG monitoring infringes at least claim 8 of the ‘641 patent, either literally or under the doctrine of equivalents, because systems including these CS products perform all the steps required in the claim, as set forth in detail in Exhibit 2. CS has published the following two documents that provide a detailed description of the use of the CS Controller and Cyber Sensor for manhole and lockbox monitoring:

- a. Cyber Sensor Installation Guide (attached as **Exhibit 8**); and
- b. CyberSecure CSS Cyber Sensor Solution (attached as **Exhibit 9**).

As shown in detail in the claim chart attached as Exhibit 2, both these documents provide support for NIS’ infringement claims.

39. CS, with knowledge of the ‘641 patent and knowledge that manhole, lockbox, and other FBG monitoring systems that include the CS Controller, Opti-Guard, and/or Cyber Sensor Products infringe the ‘641 patent, provides assistance and instruction to customers in connection with the installation and use of these CS products and the knowhow to use these CS products in

an infringing manner.

40. CS, with knowledge of the '641 patent and knowledge that FBG monitoring systems that include the CS Controller, Opti-Guard, and/or Cyber Sensor Products infringe the '641 patent, directs its salespeople and technical personnel to conduct troubleshooting and testing on monitoring systems that employ these CS products.

41. On information and belief, the CS Controller, Opti-Guard, and/or Cyber Sensor Products, when employed in FBG monitoring systems, are specifically designed for use in a manner that infringes the '641 patent, either literally or under the doctrine of equivalents, and these products have no substantially non-infringing use.

42. On information and belief, CS offers products and services that infringe the claims of the '641 patent and other NIS patents, and NIS reserves the right to pursue additional infringement in this lawsuit. These products and services include, at least, other detection systems being offered for sale and/or sold to customers for use in fiber optic network layouts arranged in a point-to-multipoint configuration.

COUNT I

(Direct Infringement of the '641 Patent)

43. NIS adopts and incorporates by reference all the foregoing allegations as if fully set forth herein.

44. CS has directly infringed and continues to directly infringe under 35 U.S.C. § 271(a) one or more claims of the '641 patent either literally and/or under the doctrine of equivalents, by making, using, selling, and/or offering for sale in the United States the Accused Products and Services that infringe one or more claims of the '641 patent.

45. CS is directly infringing the claims of the '641 patent by conducting the steps of the methods recited in the claims of the '641 patent at least when CS salespeople and technical

representatives troubleshoot and test the CS systems and methods both during and after installation at end customer facilities such as the Primary Customer data centers and DMV Facility.

46. On information and belief, CS has been aware of the '641 patent at least since the date that the parties entered into the ESR Agreement.

COUNT II
(Inducing of Infringement of the '641 Patent)

47. NIS adopts and incorporates by reference all the foregoing allegations as if fully set forth herein.

48. CS has induced infringement and continues to induce infringement under 35 U.S.C. § 271(b).

49. CS offers for sale, sells, and has sold the Accused Products and Services to entities in the networking sector including, but not limited to, the DMV Facility and the Primary Customer data centers.

50. CS's customers have directly infringed and continue to directly infringe, under 35 U.S.C. § 271(a), one or more claims of the '641 patent, either literally and/or under the doctrine of equivalents, by using the Accused Products and Services in the United States that infringe one or more claims of the '641 patent, as described in detail above.

51. CS has actively, knowingly, and intentionally induced, and continues to actively, knowingly, and intentionally induce, infringement of the '641 patent, by offering to sell, selling and/or otherwise supplying the Accused Products and Services, with the knowledge and intent that third parties will use the Accused Products and Services in the United States, for their intended purpose to infringe the '641 patent, and with the knowledge and intent to encourage and facilitate infringement through the dissemination of the Accused Products and Services and/or the creation and dissemination of documentation and technical information to customers and prospective

customers related to the Accused Products and Services.

52. CS, through its sales people and technical field representatives, over whom CS exerts control and direction, provides assistance and instruction in connection with installation and use of the Accused Product and Services at facilities and the knowhow to use the Accused Product and Services in an infringing manner, at all times having knowledge of the '641 patent and with the intent that personnel at the facilities operate the Accused Product and Services so that there is infringement of the '641 patent.

53. On information and belief, CS, through its sales people and technical field representatives, troubleshoot operation of the Accused Product and Services at customer facilities during and after installation of the Accused Product and Services with full knowledge of the '641 patent and that the Accused Product and Services operate in a manner that infringes the '641 patent and with the intent that the customers operate the Accused Product and Services in a manner that infringes the '641 patent.

54. On information and belief, CS has been aware of the '641 patent at least since the date that the parties entered into the ESR Agreement.

COUNT III
(Contributory Infringement of the '641 Patent)

55. NIS adopts and incorporates by reference all the foregoing allegations as if fully set forth herein.

56. CS offers for sale, sells, and has sold the Accused Products and Services to entities in the networking sector including, but not limited to, the DMV Facility and the Primary Customer data centers.

57. CS's customers have directly infringed and continue to directly infringe, under 35 U.S.C. § 271(a), one or more claims of the '641 patent, either literally and/or under the doctrine of

equivalents, by using the Accused Products and Services in the United States that infringe one or more claims of the '641 patent, as described in detail above.

58. CS has contributed and continues to contribute to the infringement by third parties, including its customers, of one or more claims of the '641 patent under 35 U.S.C. § 271(c), by selling and/or offering for sale in the United States the Accused Products and Services knowing that those products and services constitute a material part of the inventions of the '641 patent, knowing that those products and services are especially made or adapted to infringe the '641 patent, and knowing that when sold for use with a point-to-multipoint network layout those products are not staple articles of commerce suitable for substantial non-infringing use.

59. CS, through its sales people and technical field representatives, over whom CS exerts control and direction, provides assistance and instruction in connection with installation and use of the Accused Product and Services at facilities and the knowhow to use the Accused Product and Services in an infringing manner at all times having knowledge of the '641 patent and with the intent that personnel at the facilities operate the Accused Product and Services so that there is infringement of the '641 patent.

60. On information and belief, CS, through its sales people and technical field representatives, troubleshoot operation of the Accused Product and Services at customer facilities during and after installation of the Accused Product and Services with full knowledge of the '641 patent and that the Accused Product and Services operate in a manner that infringes the '641 patent and with the intent that the customers operate the Accused Product and Services in a manner that infringes the '641 patent.

61. The Accused Products and Services are designed in a manner that infringe one or more claims of the '641 patent, and the Accused Products and Services when sold for use with a

point-to-multipoint network layout are not staple articles of commerce suitable for substantial non-infringing use.

62. On information and belief, CS has been aware of the '641 patent at least since the date that the parties entered into the ESR Agreement.

CS WILLFULLY INFRINGES THE '641 PATENT

63. NIS adopts and incorporates by reference all the foregoing allegations as if fully set forth herein.

64. On information and belief, CS has been aware of the '641 patent at least since the date that the parties entered into the ESR Agreement in 2015. Despite this knowledge, and an objectively high likelihood that its actions constitute direct and other infringement of the '641 patent, CS has engaged in infringement of the '641 patent.

65. CS has sought to replace NIS products with its own products thereby ensuring that the resulting CS optical fiber intrusion monitoring system and method would infringe the '641 patent.

66. The infringing conduct by CS of the '641 patent renders this case exceptional within the meaning of 35 U.S.C. § 285.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Network Integrity Systems, Inc. respectfully requests that this Court enter judgment against Defendant CyberSecure IPS LLC:

- A. That Defendant has directly infringed the patent-in-suit;
- B. That Defendant has induced infringement of the patent-in-suit;
- C. That Defendant has contributed to infringement of the patent-in-suit;
- D. That Plaintiff be awarded all damages adequate to compensate it for Defendant's

infringement of the patent-in-suit, such damages to be determined by a jury with pre-judgment and post-judgment interest;

E. That Defendant's infringement was willful and that such damages be trebled pursuant to 35 U.S.C. § 284;

F. For an order permanently enjoining Defendant and its officers, agents, servants and employees, privies, and all persons in concert or participation with it, from further infringement of the patent-in-suit;

G. That this case be declared an exceptional case within the meaning of 35 U.S.C. § 285 and that Plaintiff be awarded its attorney's fees, costs and expenses incurred relating to this action; and

H. That Plaintiff be awarded such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all claims so triable.

Dated: April 7, 2025

Respectfully submitted,

/s/ Joseph L. Meadows
Joseph L. Meadows (VA Bar No. 92729)
Howard N. Shipley (VA Bar No. 40527)
GORDON REES SCULLY MANSUKHANI, LLP
277 S Washington Street, Suite 550
Alexandria, VA 22314
T: 202-399-1009
F: 202-800-2999
jmeadows@grsm.com
hshipley@grsm.com

Counsel for Plaintiff

VERIFICATION

I declare under penalty of perjury, to the best of my knowledge, information and belief, that the contents of this Complaint are true and accurate.

Dated: April 7, 2025

A handwritten signature in black ink, appearing to read 'Dave Cunningham', with a long horizontal flourish extending to the right.

Dave Cunningham
President
Network Integrity Systems, Inc.

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

NETWORK INTEGRITY SYSTEMS, INC.

(b) County of Residence of First Listed Plaintiff CATAWBA (NC)
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Joe Meadows & Howard Shipley, Gordon Rees, 277 S.
Wash. St., Ste. 550, Alex., VA 22314, 202-399-1009

DEFENDANTS

CYBERSECURE IPS LLC

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF
THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff ☒ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|----------------------------|----------------------------|---|----------------------------|----------------------------|
| Citizen of This State | ☐ 1 | ☐ 1 | Incorporated or Principal Place of Business In This State | ☐ 4 | ☐ 4 |
| Citizen of Another State | ☐ 2 | ☐ 2 | Incorporated and Principal Place of Business In Another State | ☐ 5 | ☐ 5 |
| Citizen or Subject of a Foreign Country | ☐ 3 | ☐ 3 | Foreign Nation | ☐ 6 | ☐ 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
☐ 110 Insurance ☐ 120 Marine ☐ 130 Miller Act ☐ 140 Negotiable Instrument ☐ 150 Recovery of Overpayment & Enforcement of Judgment ☐ 151 Medicare Act ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans) ☐ 153 Recovery of Overpayment of Veteran's Benefits ☐ 160 Stockholders' Suits ☐ 190 Other Contract ☐ 195 Contract Product Liability ☐ 196 Franchise	PERSONAL INJURY ☐ 310 Airplane ☐ 315 Airplane Product Liability ☐ 320 Assault, Libel & Slander ☐ 330 Federal Employers' Liability ☐ 340 Marine ☐ 345 Marine Product Liability ☐ 350 Motor Vehicle ☐ 355 Motor Vehicle Product Liability ☐ 360 Other Personal Injury ☐ 362 Personal Injury - Medical Malpractice	PERSONAL INJURY ☐ 365 Personal Injury - Product Liability ☐ 367 Health Care/Pharmaceutical Personal Injury Product Liability ☐ 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY ☐ 370 Other Fraud ☐ 371 Truth in Lending ☐ 380 Other Personal Property Damage ☐ 385 Property Damage Product Liability	☐ 625 Drug Related Seizure of Property 21 USC 881 ☐ 690 Other LABOR ☐ 710 Fair Labor Standards Act ☐ 720 Labor/Management Relations ☐ 740 Railway Labor Act ☐ 751 Family and Medical Leave Act ☐ 790 Other Labor Litigation ☐ 791 Employee Retirement Income Security Act IMMIGRATION ☐ 462 Naturalization Application ☐ 465 Other Immigration Actions	☐ 422 Appeal 28 USC 158 ☐ 423 Withdrawal 28 USC 157 INTELLECTUAL PROPERTY RIGHTS ☐ 820 Copyrights ☒ 830 Patent ☐ 835 Patent - Abbreviated New Drug Application ☐ 840 Trademark ☐ 880 Defend Trade Secrets Act of 2016 SOCIAL SECURITY ☐ 861 HIA (1395ff) ☐ 862 Black Lung (923) ☐ 863 DIWC/DIWW (405(g)) ☐ 864 SSID Title XVI ☐ 865 RSI (405(g)) FEDERAL TAX SUITS ☐ 870 Taxes (U.S. Plaintiff or Defendant) ☐ 871 IRS—Third Party 26 USC 7609	☐ 375 False Claims Act ☐ 376 Qui Tam (31 USC 3729(a)) ☐ 400 State Reapportionment ☐ 410 Antitrust ☐ 430 Banks and Banking ☐ 450 Commerce ☐ 460 Deportation ☐ 470 Racketeer Influenced and Corrupt Organizations ☐ 480 Consumer Credit (15 USC 1681 or 1692) ☐ 485 Telephone Consumer Protection Act ☐ 490 Cable/Sat TV ☐ 850 Securities/Commodities/Exchange ☐ 890 Other Statutory Actions ☐ 891 Agricultural Acts ☐ 893 Environmental Matters ☐ 895 Freedom of Information Act ☐ 896 Arbitration ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision ☐ 950 Constitutionality of State Statutes
REAL PROPERTY ☐ 210 Land Condemnation ☐ 220 Foreclosure ☐ 230 Rent Lease & Ejectment ☐ 240 Torts to Land ☐ 245 Tort Product Liability ☐ 290 All Other Real Property	CIVIL RIGHTS ☐ 440 Other Civil Rights ☐ 441 Voting ☐ 442 Employment ☐ 443 Housing/Accommodations ☐ 445 Amer. w/Disabilities - Employment ☐ 446 Amer. w/Disabilities - Other ☐ 448 Education	PRISONER PETITIONS Habeas Corpus: ☐ 463 Alien Detainee ☐ 510 Motions to Vacate Sentence ☐ 530 General ☐ 535 Death Penalty Other: ☐ 540 Mandamus & Other ☐ 550 Civil Rights ☐ 555 Prison Condition ☐ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District (specify) ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
35 U.S.C. Sections 271 and 285
Brief description of cause:
direct, induced, contributory, and willful infringement of U.S. Patent No. 7,706,641

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. **DEMAND \$** _____ CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE _____ DOCKET NUMBER _____

DATE

SIGNATURE OF ATTORNEY OF RECORD

4/7/2025

/s/ Joseph L. Meadows

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

EX-2005
Page 18

Case 8:25-cv-01974-TDC Document 1-1 Filed 04/07/25 Page 2 of 2
INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
 - (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
 - (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
- Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
- Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
- Original Proceedings. (1) Cases which originate in the United States district courts.
- Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
- Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
- Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
- Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
- Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
- Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
- PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
- Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
- Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related cases, if any. If there are related cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

EXHIBIT 1

(12) **United States Patent**
Murphy et al.

(10) **Patent No.:** **US 7,706,641 B2**
(45) **Date of Patent:** **Apr. 27, 2010**

(54) **MONITORING INDIVIDUAL FIBERS OF AN OPTICAL CABLE FOR INTRUSION**

(75) Inventors: **Cary R. Murphy**, Hickory, NC (US);
Mark K. Bridges, Hickory, NC (US);
Joseph Giovanni, Conover, NC (US);
David E. Vokey, Sidney (CA); **Daniel M. Goertzen**, Winnipeg (CA)

(73) Assignee: **Network Integrity Systems, Inc.**,
Hickory, NC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 516 days.

(21) Appl. No.: **11/461,917**

(22) Filed: **Aug. 2, 2006**

(65) **Prior Publication Data**

US 2007/0086694 A1 Apr. 19, 2007

Related U.S. Application Data

(60) Provisional application No. 60/704,926, filed on Aug. 3, 2005.

(51) **Int. Cl.**
G02B 6/00 (2006.01)

(52) **U.S. Cl.** **385/13; 385/12**

(58) **Field of Classification Search** **385/13**
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,026,141 A * 6/1991 Griffiths 385/13

5,134,386 A * 7/1992 Swanic 340/541
5,680,104 A * 10/1997 Slemon et al. 340/568.2
5,809,185 A * 9/1998 Mitchell 385/12
6,967,584 B2 * 11/2005 Maki 340/657
7,211,783 B2 * 5/2007 Beinhocker 250/227.14
2004/0071382 A1 * 4/2004 Rich et al. 385/12
2004/0114888 A1 * 6/2004 Rich et al. 385/101

* cited by examiner

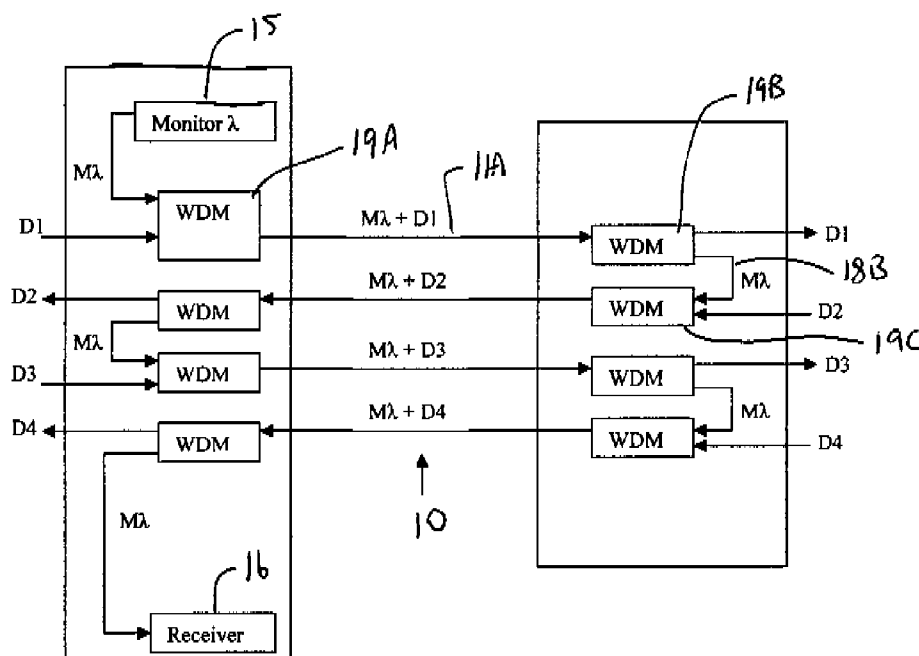
Primary Examiner—Michelle R Connelly Cushwa

(74) *Attorney, Agent, or Firm*—Adrian D. Battison; Ade & Company Inc.

(57) **ABSTRACT**

Some or all of the optical fibers of a single-mode or multi-mode cable are monitored for intrusion by transmitting through the fibers a signal which can be analyzed for changes in its characteristics which are indicative of movement as a prelude to an intrusion event. To avoid independent monitors of all of the fibers, in some cases the same light signal is looped through a plurality of the fibers in series by passive jumpers. Switches can be used to disconnect out those fibers which are compromised. As an alternative a plurality of separate monitoring signals can be provided each associated with its own sensor where unique combinations of the signals are transmitted through separate fibers allowing a higher number of fibers to be monitored than the number of signals.

16 Claims, 6 Drawing Sheets



U.S. Patent

Apr. 27, 2010

Sheet 1 of 6

US 7,706,641 B2

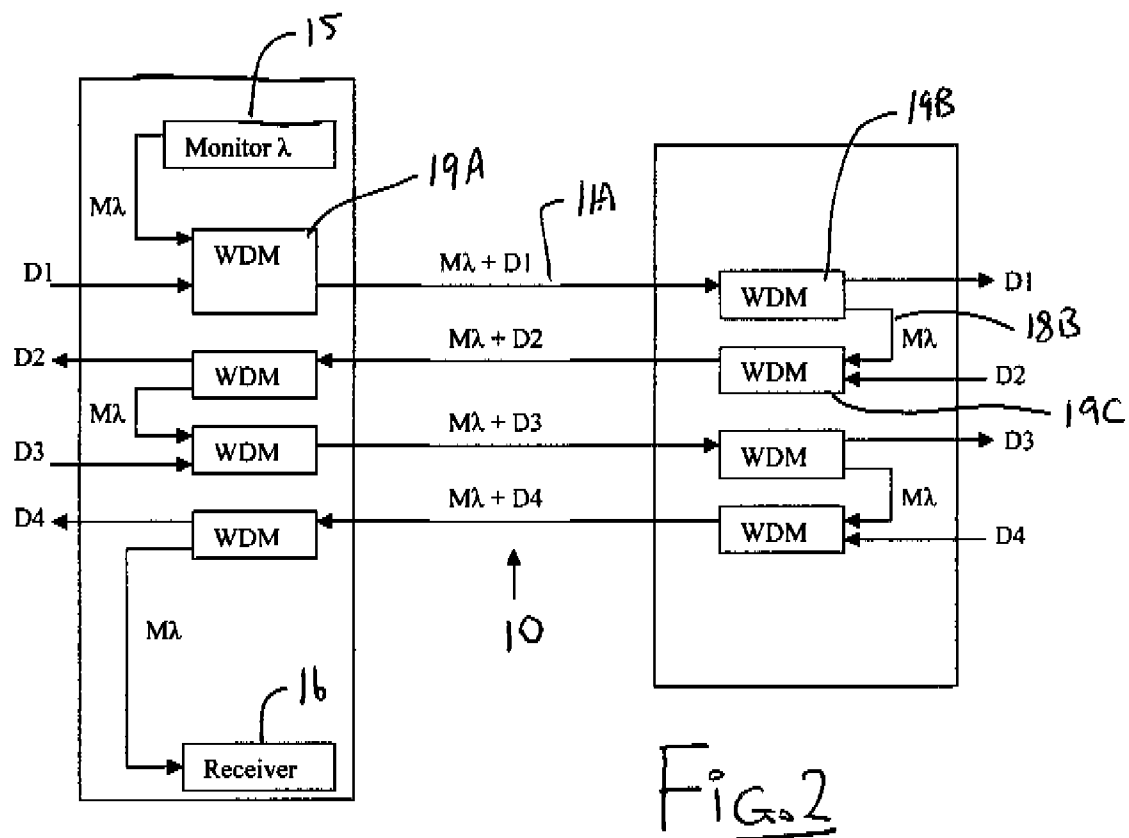
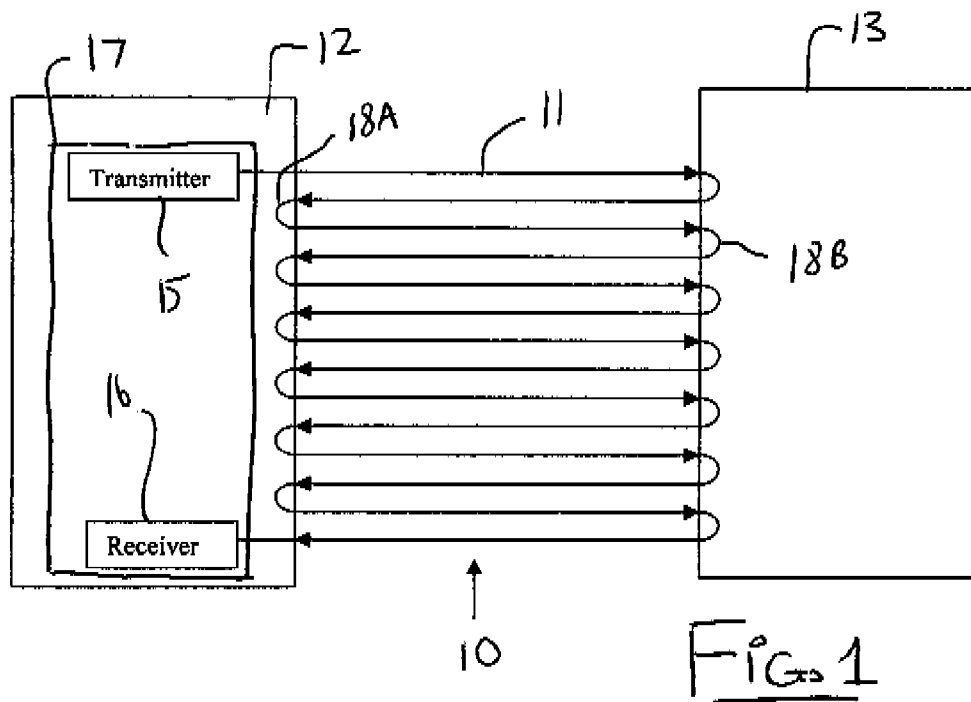
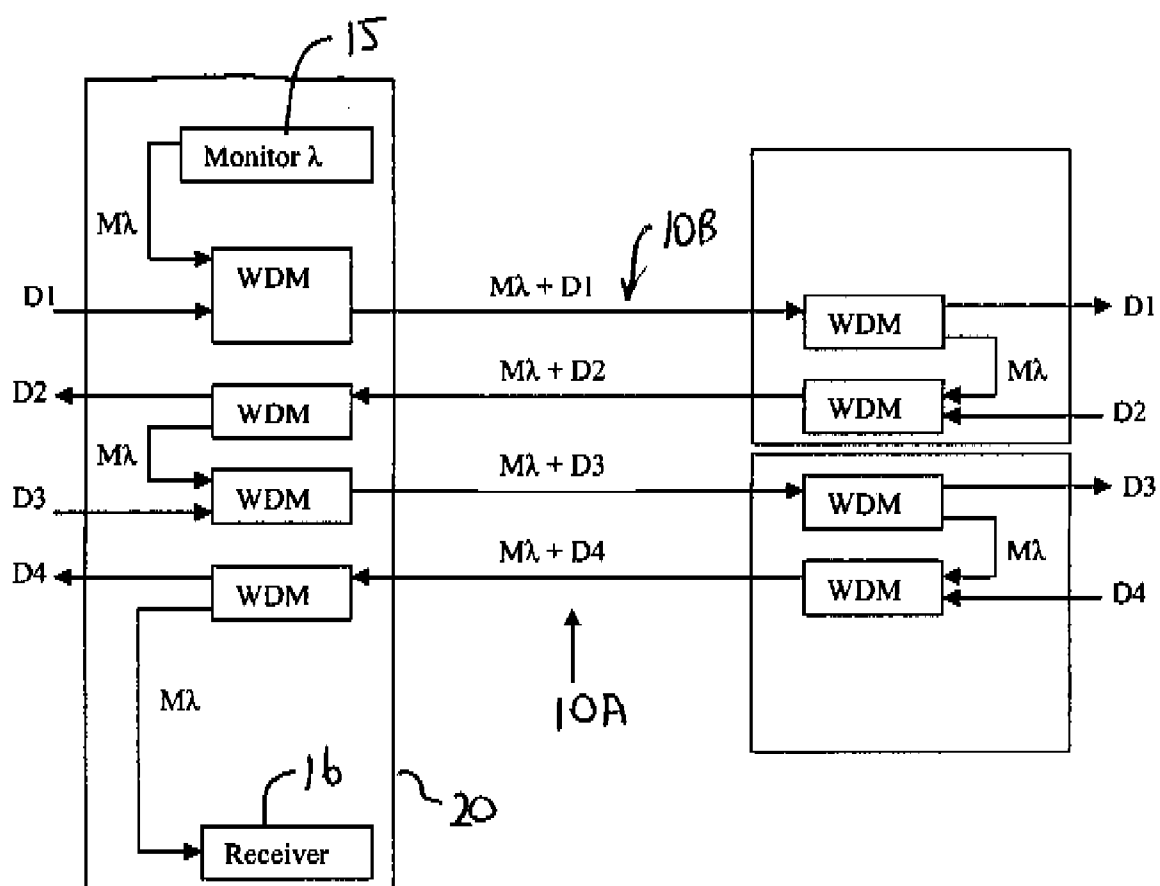


FIG 3

U.S. Patent

Apr. 27, 2010

Sheet 3 of 6

US 7,706,641 B2

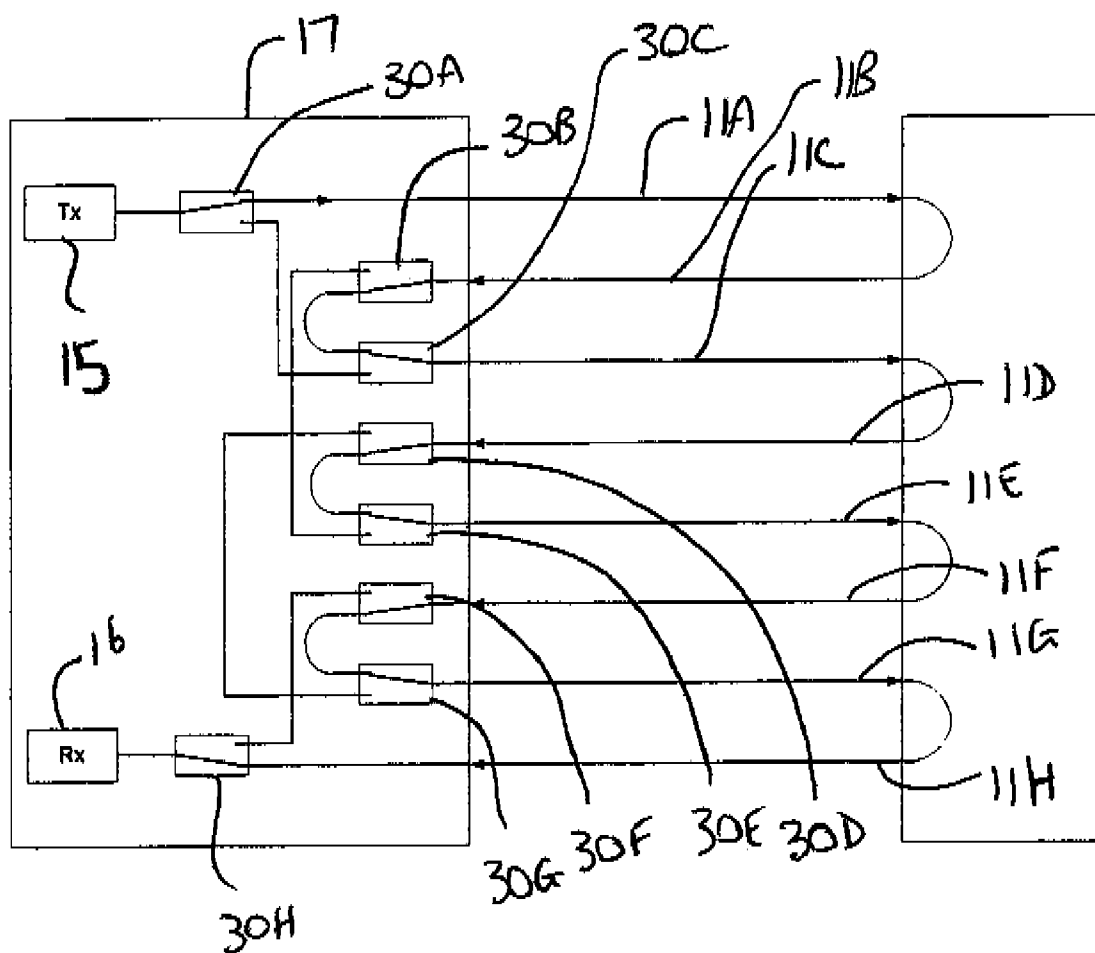


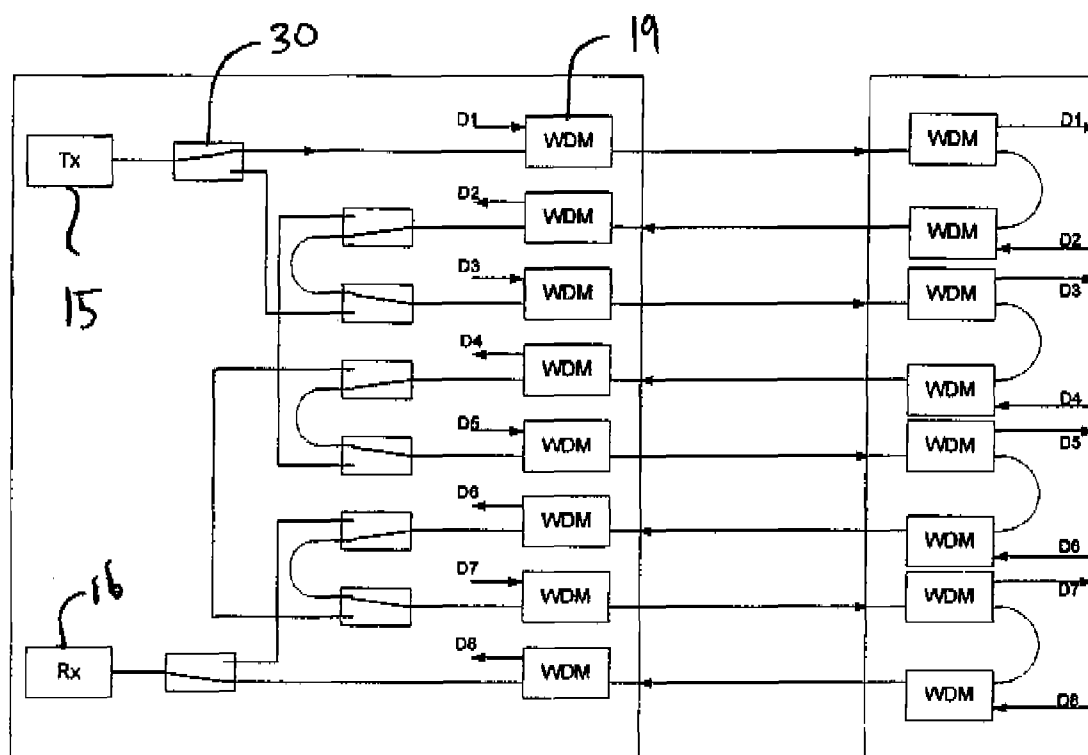
Fig. 4

U.S. Patent

Apr. 27, 2010

Sheet 4 of 6

US 7,706,641 B2



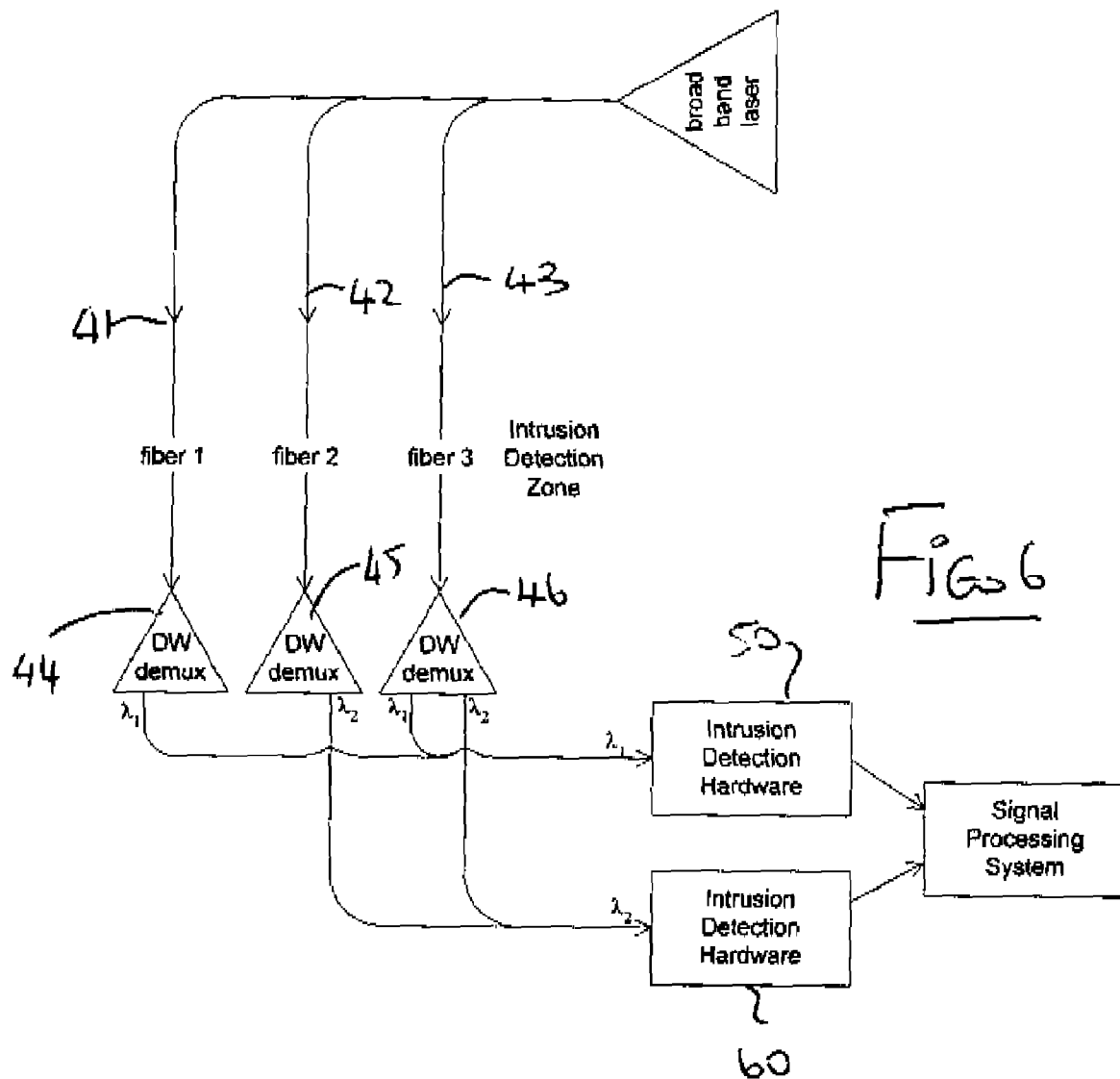
Figs

U.S. Patent

Apr. 27, 2010

Sheet 5 of 6

US 7,706,641 B2



U.S. Patent

Apr. 27, 2010

Sheet 6 of 6

US 7,706,641 B2

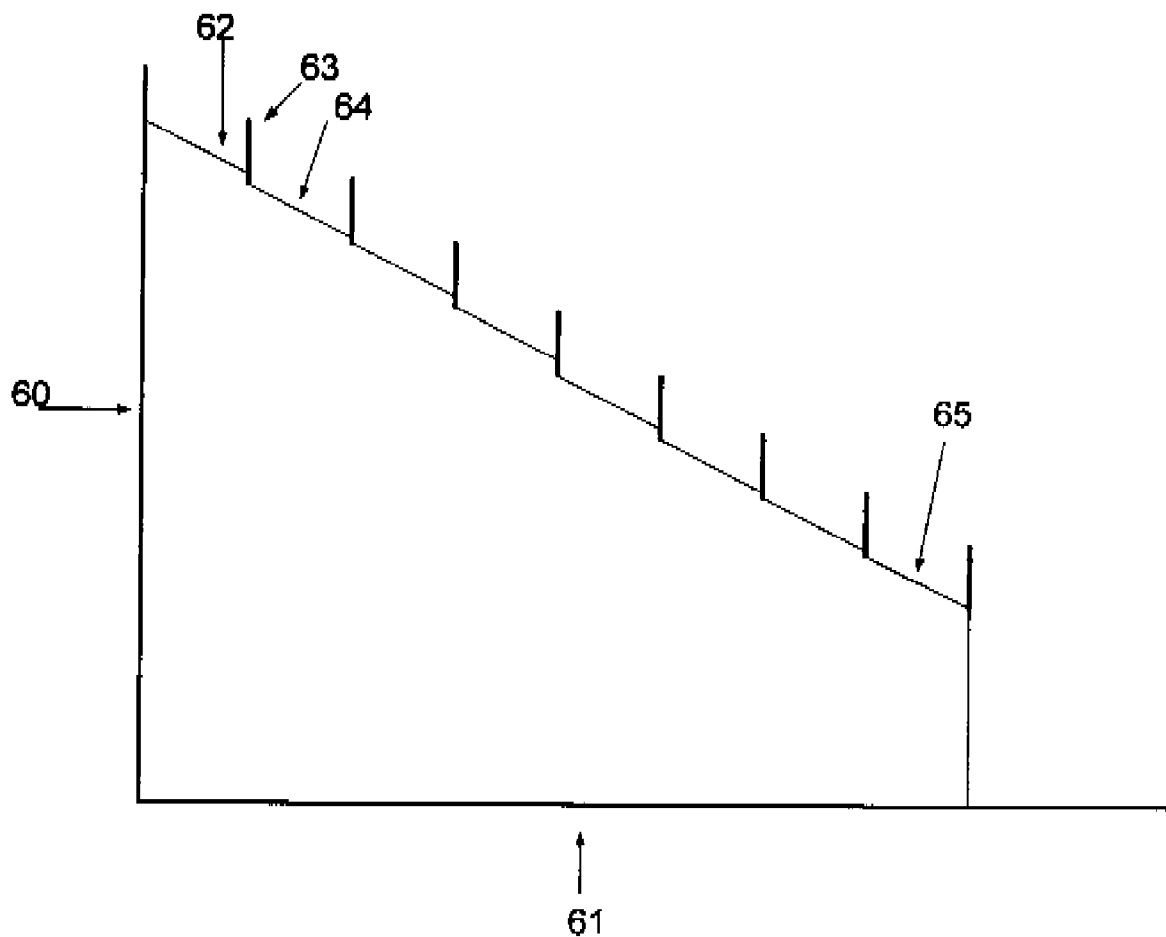


FIG. 7

US 7,706,641 B2

1

MONITORING INDIVIDUAL FIBERS OF AN OPTICAL CABLE FOR INTRUSION

This application claims the benefit of the priority date under 35USC119 from Provisional Application 60/704,926 filed 3 Aug. 2005.

This invention relates to a method of monitoring at least some of the individual fibers of an optical cable for intrusion.

BACKGROUND OF THE INVENTION

In the following patent applications all filed Jun. 15, 2005 of the present applicant are disclosed and claimed techniques for monitoring single mode fibers for intrusion:

Application Ser. No. 11/152,679 entitled AN INTRUSION DETECTION SYSTEM FOR USE ON SINGLE MODE OPTICAL FIBER USING FRESNEL REFLECTIONS.

Application Ser. No. 11/152,772 entitled AN INTRUSION DETECTION SYSTEM FOR USE ON SINGLE MODE OPTICAL FIBER USING A STORAGE REGISTER FOR DATA.

Application Ser. No. 11/152,680 entitled AN INTRUSION DETECTION SYSTEM FOR USE ON SINGLE MODE OPTICAL FIBER USING A SIMPLIFIED POLARIMETER.

Application Ser. No. 11/152,663 entitled AN INTRUSION DETECTION SYSTEM FOR USE ON SINGLE MODE OPTICAL FIBER USING A COST REDUCED POLARIMETER.

Application Ser. No. 11/152,681 entitled AN INTRUSION DETECTION SYSTEM FOR USE ON SINGLE MODE OPTICAL FIBER USING A POLARIMETER.

In the following patent applications both filed May 26, 2005 of the present applicant are disclosed and claimed techniques for monitoring multi-mode fibers for intrusion:

Application Ser. No. 11/137,776 entitled AN INTRUSION DETECTION SYSTEM FOR USE ON AN OPTICAL FIBER USING A TRANSLATOR OF TRANSMITTED DATA FOR OPTIMUM MONITORING CONDITIONS.

Application Ser. No. 11/137,777 entitled AN INTRUSION DETECTION SYSTEM FOR USE ON MULTI-MODE OPTICAL FIBER USING AN OFFSET LAUNCH AND TAP COUPLER.

Reference is also made to the following application filed on the same day as this application which is application Ser. No. 11/461,661 under entitled AN INTRUSION DETECTION AND LOCATION SYSTEM FOR USE ON MULTIMODE FIBER OPTIC CABLE

The disclosures of all of the above applications are incorporated herein by reference.

Using the techniques disclosed above, in physical layer intrusion detection, one factor to be considered in protecting a multi-fiber cable is the choice of how many fiber strands to protect. On one hand, a single fiber or fiber pair will protect the cable somewhat, and at a reduced price. At the other extreme, an IDS system per fiber can be quite costly.

SUMMARY OF THE INVENTION

It is one object of the present invention to provide an improved method of monitoring fibers of a cable.

According to the invention there is provide a method for detecting movement of optical fibers of an optical fiber cable comprising:

providing a optical fiber cable having a first end and a second end, the cable having a plurality of fibers;

2

monitoring a plurality of fibers of the cable by detecting movement at locations along the length thereof by:

providing at least one source of light for injection onto the fibers;

providing at least one sensor arrangement for receiving light transmitted through the fibers;

injecting light from the at least one source into one end of the each of the fibers to be monitored;

in the at least one sensor arrangement, detecting a series of received light signals which have been transmitted along the fibers;

in the at least one sensor arrangement, comparing at least some of the received light signals relative to data obtained from previously received ones of the received light signals to detect changes in the received light signals relative to the previously received light signals;

in the at least one sensor arrangement, analyzing the changes to determine any changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;

generating an alarm in response to the detection of any such changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;

and using optical communication components to communicate light from the at least one source to more than one of the fibers and to communicate light from more than one of the fibers to the at least one sensor arrangement such that the number of fibers monitored is greater than the number of sources and greater than the number of sensor arrangements.

Preferably there is provided at least one jumper connected between a first and a second fibers so as to loop the monitor light exiting from the first fiber into the second fiber so as to use in monitoring the first and second fibers a common single source.

Preferably there is provided at a first end of the cable a plurality of jumpers each connected between an exit end of a first fiber and an entry end of a next fiber fibers so as to loop the monitor light exiting from the first fiber into the next fiber and there is provided at a second end of the cable a second plurality of jumpers each connected between an exit end of a next fiber and an entry end of a subsequent fiber fibers so as to loop the monitor light exiting from the next fiber into the subsequent fiber such that the light from a common single source passes thorough each fiber sequentially.

Preferably the source and the sensing arrangement are arranged at a first end of the cable and at the second end of the cable is provided a passive unit forming the series of jumpers defining the communication components.

Preferably there is provided a single source and a single sensing arrangement and the monitored fibers are treated as one fiber therebetween.

Preferably the sensing arrangement includes locating arrangement for detecting the location of a detected movement and there is provided a stored table of fiber lengths which allows the sensing arrangement to determine which fiber was is moved.

Preferably there is provided a plurality of wavelength division multiplexers (WDMs) such that each monitored fiber has connected thereto at an entry end and an exit end a respective pair of the WDMs for separating the light from the source from a data signal transmitted simultaneously with the monitoring light through the fiber.

Preferably all transmission on monitored cable is the monitor wavelength of the light source multiplexed to the data wavelength.

US 7,706,641 B2

3

Preferably all loop-backs between WDMs is at the monitor wavelength.

Preferably there is provided a plurality of cables arranged in a hub-and-spoke arrangement where a main unit in a central location feeds remote units and wherein the fibers of more than one of the cable are monitored.

Preferably there is provided a plurality of optical switches each arranged at a respective end of a respective fiber.

Preferably the optical switches are arranged to break the circuit of a pair of fibers in the event that a movement is detected.

Preferably the optical switches are arranged to redirect the monitor wavelength round a fiber pair, thereby bypassing a broken link.

Preferably the optical switches are arranged to scan fibers to identify which one has been intruded, precluding the need for locating.

As an alternative method, there is provided for the plurality of fibers a second plurality of independent monitoring signals each of which can be separated from the others wherein the number of signals is less than the number of fibers, each monitoring signal being associated with a respective sensing arrangement.

In this alternative method, there may be provided multiplexing devices arranged such that each of the fibers to be monitored has launched therein a unique combination of one or more of the independent monitoring signals.

Thus in one arrangement, the invention solves this by allowing a single IDS unit with additional distal-end optics to monitor some or all of the fibers in a cable at a reduced cost.

This invention allows for the monitoring all of the fibers in a cable using a loop-back technique. When used with a locating IDS system, individual fibers can be identified. When used with optical switches, compromised fibers can be eliminated from the data path.

BRIEF DESCRIPTION OF THE DRAWINGS

One embodiment of the invention will now be described in conjunction with the accompanying drawings in which:

FIG. 1 shows schematically a system according to the present invention using a dark fiber.

FIG. 2 shows schematically a system according to the present invention using an active fiber.

FIG. 3 shows schematically a system according to the present invention using a hub and spoke arrangement.

FIG. 4 shows schematically a system similar to that of FIG. 1 according to the present invention using a dark fiber where there are provided switches for controlling the connection of the fibers.

FIG. 5 shows schematically a system similar to that of FIG. 2 according to the present invention using an active fiber where there are provided switches for controlling the connection of the fibers.

FIG. 6 shows schematically an alternative system where a broadband laser source is communicated to a series of the fibers of a cable and there are provided dense wave demultiplexers for extracting different signals from different ones of the fibers.

FIG. 7 shows a trace of an OTDR modified for intrusion detection where each of the loops of fiber are illustrated by a section of the trace. In the drawings like characters of reference indicate corresponding parts in the different figures.

DETAILED DESCRIPTION

In FIG. 1 is shown a cable 10 formed by a series of fibers 11 and connecting from a first end connection system 12 at one

4

end of the cable to a second end connection system 13 at the second remote end of cable. At the first end is provided a monitoring system 17 including a transmitter 15 of light signals which are communicated to a receiver 16 after passing through one or more fibers.

The fibers can be single mode fibers or multi-mode fibers and can use the techniques described in one or more of the above applications to provide monitoring of movement of the fiber indicative of an intrusion event. The disclosure of the above applications are incorporated herein by reference to provide full details of the various techniques available. Other techniques can also be used.

Internal to the monitoring equipment is a series of jumpers 18A at the transmit or first end and 18B at the distal end, with which to loop the monitor light back into the next fiber. At the distal end, a passive unit 13 consisting of a mirror set of loops 18B completes the circuit. The monitoring equipment treats the cable as one fiber. If the monitoring equipment is capable of event location using the techniques described in one or more of the above applications, a stored table of fiber lengths would allow such a device to determine which fiber was compromised.

Thus the arrangement describer herein uses optical communication components to communicate light from the at least one source to more than one of the fibers and to communicate light from more than one of the fibers to the at least one sensor arrangement such that the number of fibers monitored is greater than the number of sources and greater than the number of sensor arrangements.

A similar system is shown in FIG. 2 which uses internal wavelength division multiplexers (WDMs) 19A at the transmit first end and WDMs 19B at the remote end.

Thus a first fiber 11A is connected to a WDM 19A at its transmit end so as to receive thereon a monitor signal Mλ which is multiplexed with a data signal D1. At the remote end the multiplexed signal is separated by the WDM 19B to extract the data signal D1 and the monitor signal Mλ which is looped back using the jumper 18B. The looped back monitoring signal is again multiplexed at the WDM 19C with data signal D2. The remaining fibers of the cable are symmetrically monitored and may carry data using the arrangement generally described above in the same symmetrical manner and using the same monitoring signal Mλ. All transmission on monitored cable is the monitor wavelength multiplexed to the data wavelength. All loop-backs between WDMs is at the monitor wavelength. All signals shown entering and leaving the boxes are data at the data wavelength.

As shown in FIG. 3 the method can also be used in a hub-and-spoke situation where a main unit 20 in a central location feeds remote units 21 and 22 over cables 10A and 10B. This can be used in a server and computer set up such as in an office environment.

Turning now to FIG. 4 there is shown a further embodiment substantially identical to that of FIG. 1 but with the addition of optical switches 30. In this series of embodiments, the optical switches 30 can be used to:

1. Break the circuit of the intruded fiber pair;
2. Redirect the monitor wavelength round a fiber pair, thereby bypassing a broken link; and/or
3. Scan fibers to identify which one has been intruded, precluding the need for locating hardware.

Thus the transmitter 15 is connected to a first optical switch 30A which can switch between two paths feeding the first fiber 11A or the third fiber 11C. At the third fiber 11C is provided a switch 30C which allows the third fiber to select signals from either the transmitter 15 or the second fiber 11B. The fibers 11D, 11E, 11F, 11G, and 11H are connected sym-

US 7,706,641 B2

5

metrically relative to the switches **30D**, **30E**, **30F**, **30G**, and **30H**. In this way, for example the switches **30A** and **30C** can be operated to break the circuit defined by the fiber pair **11A** and **11B**. In this way, for example the switches **30A**, **30C** and **30D** can be operated to redirect the monitor wavelength round the fiber pair **11A** and **11B** by using the fiber pair **11C** and **11D**. In this way, for example by operating the switches in pairs, the monitoring signal can be communicated through selected ones of the pairs of fibers to determine which are compromised.

FIG. **5** is shown an arrangement which uses both the switches **30** and the WDMs **19** for use of the system described above in relation to FIG. **4** on an active cable system as shown and described in relation to FIG. **2**.

Turning now to FIG. **6** there is shown an alternative arrangement. The merit of this design is to be able to monitor N fibers with only $\log 2 (N+1)$ detectors. For example:

detectors	fibers
1	1
2	3
3	7
4	15
5	31
10	1023

There is provided a broadband laser **40** which generates light at a required number of wavelengths equal to the number of detectors so that in the example shown there are two wavelengths λ_1 and λ_2 and two detectors **50** and **60**. In the example in the above table where there are 3 detectors there will of course be three wavelengths monitored by those detectors.

Each of the fibers **41**, **42** and **43** supplies an output to a respective one of three Dense Wave Demultiplexors **44**, **45** and **46** which extract wavelengths λ_1 and λ_2 from the broadband signal.

There is an Intrusion Detection Hardware unit **50**, **60** for each received wavelength. As explained hereinbefore the Intrusion Detection Hardware units may monitor multi-mode or single mode fibers using the techniques described in one of more of the above patent applications. Each wavelength is independently monitored looking for characteristics indicative of movement of the fiber as described in the above applications.

The signal processing system determines which fiber an event has occurred on by examining activity of the wavelength inputs. If an event occurs only at wavelength λ_1 , the system attributes the event to fiber **41** because the Demultiplexor **44** is the only one which extracts signals which relate only to wavelength λ_1 . If an event occurs only on λ_2 , the system attributes the event to fiber **42** because the Demultiplexor **45** is the only one which extracts signals which relate only to wavelength λ_2 . If it occurs on both λ_1 and λ_2 simultaneously, the system attributes the event to fiber **43** because the Demultiplexor **46** is the only one which extracts signals which relate both to wavelengths λ_1 and λ_2 . It will be appreciated that this scheme can be extrapolated to three or more sensing systems and three or more wavelengths.

In this way there is provided for the plurality of fibers a second plurality of independent monitoring signals λ_1 and λ_2 each of which can be separated from the others by the Demultiplexors, where the number of signals is less than the number of fibers **41**, **42** **43**, each monitoring signal λ_1 and λ_2 being associated with a respective sensing arrangement **50**, **60**.

6

Thus there multiplexing devices arranged such that each of the fibers to be monitored has detected therefrom a unique combination of one or more of the independent monitoring signals, that is λ_1 , λ_2 , and combined λ_1 and λ_2 .

Turning now to FIG. **7** is shown the representative trace of an Optical Time Domain Reflectometer (OTDR) which has been modified for intrusion detection. The horizontal axis **61** represents distance in an OTDR, vertical axis **60** represents signal level. Trace portion **62** shows the loss of the first fiber, reflection **63** is representative of the interface between the distal end of fiber one and the distal end of fiber 2. Portion **64** represents fiber 2, however the fiber characteristics are displayed reversed in time as the light is launched into the distal end travelling toward the near end. This pattern continues N times to the final section **65**. Using analysis software, the system can identify which fiber has experienced a perturbation by detecting which segment on the virtual modified OTDR trace.

Since various modifications can be made in my invention as herein above described, and many apparently widely different embodiments of same made within the spirit and scope of the claims without departure from such spirit and scope, it is intended that all matter contained in the accompanying specification shall be interpreted as illustrative only and not in a limiting sense.

The invention claimed is:

1. A method for detecting movement of optical fibers of an optical fiber cable comprising:

providing a optical fiber cable having a first end and a second end, the cable having a plurality of fibers each of which extends from the first end to the second end;

monitoring a plurality of fibers of the cable by detecting movement of the fiber at locations along the length of the fiber by:

providing at least one source of light for injection onto the fibers;

providing at least one sensor arrangement for receiving light transmitted through the fibers;

injecting light from the at least one source into one end of each of the fibers to be monitored;

in the at least one sensor arrangement, detecting a series of received light signals which have been transmitted along the fibers to be monitored;

in the at least one sensor arrangement, comparing at least some of the received light signals relative to data obtained from previously received ones of the received light signals to detect changes in the received light signals relative to the previously received light signals;

in the at least one sensor arrangement, analyzing the changes to determine any changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;

generating an alarm in response to the detection of any such changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;

and using optical communication components to communicate light from the at least one source to more than one of the fibers of the optical fiber cable and to communicate light from more than one of the fibers of the optical fiber cable to the at least one sensor arrangement such that the number of fibers of the optical fiber cable monitored is greater than the number of sources and greater than the number of sensor arrangements.

2. The method according to claim **1** wherein the light is injected from the at least one source into said one end of a first of the fibers to be monitored at the first end of the cable and

US 7,706,641 B2

7

wherein there is provided at least one jumper at the second end of the cable connected between the first fiber of the optical fiber cable and a second fiber of the optical fiber cable so as to loop the monitor light exiting from the first fiber into the second fiber so as to use in monitoring the first and second fibers said at least one source as a common single source.

3. The method according to claim 1 wherein there is provided at the first end of the cable a plurality of jumpers each connected between an exit end of a first fiber and an entry end of a next fiber so as to loop the monitor light exiting from the first fiber into the next fiber and wherein there is provided at the second end of the cable a second plurality of jumpers each connected between an exit end of a next fiber and an entry end of a subsequent fiber so as to loop the monitor light exiting from the next fiber into the subsequent fiber such that the light from a common single source passes thorough each fiber sequentially.

4. The method according to claim 3 wherein the source and the sensing arrangement are arranged at a first end of the cable and at the second end of the cable is provided a passive unit forming the series of jumpers defining the communication components.

5. The method according to claim 3 wherein there is provided a single source and a single sensing arrangement and wherein the monitored fibers are treated as one fiber therebetween.

6. The method according to claim 1 wherein there is provided for the plurality of fibers a second plurality of independent monitoring signals each of which can be separated from the others wherein the number of signals is less than the number of fibers, each monitoring signal being associated with a respective sensing arrangement.

7. The method according to claim 6 wherein there are provided multiplexing devices arranged such that each of the fibers to be monitored has detected therefrom a unique combination of one or more of the independent monitoring signals.

8. A method for detecting movement of optical fibers comprising:

providing at least one source of light for injection onto the fibers;

providing at least one sensor arrangement for receiving light transmitted through the fibers;

injecting light from the at least one source into one end of each of the fibers to be monitored;

in the at least one sensor arrangement, detecting a series of received light signals which have been transmitted along the fibers;

in the at least one sensor arrangement, comparing at least some of the received light signals relative to data obtained from previously received ones of the received light signals to detect changes in the received light signals relative to the previously received light signals;

in the at least one sensor arrangement, analyzing the changes to determine any changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;

generating an alarm in response to the detection of any such changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;

and using optical communication components to communicate light from the at least one source to more than one of the fibers and to communicate light from more than one of the fibers to the at least one sensor arrangement

8

such that the number of fibers monitored is greater than the number of sources and greater than the number of sensor arrangements;

wherein the at least one sensing arrangement includes a locating arrangement for detecting the location of a detected movement and wherein there is provided a stored table of fiber lengths of the plurality of fibers which allows the at least one sensing arrangement to determine which fiber of the plurality of fibers has moved.

9. A method for detecting movement of optical fibers comprising:

providing at least one source of light for injection onto the fibers;

providing at least one sensor arrangement for receiving light transmitted through the fibers;

injecting light from the at least one source into one end of each of the fibers to be monitored;

in the at least one sensor arrangement, detecting a series of received light signals which have been transmitted along the fibers;

in the at least one sensor arrangement comparing at least some of the received light signals relative to data obtained from previously received ones of the received light signals to detect changes in the received light signals relative to the previously received light signals;

in the at least one sensor arrangement, analyzing the changes to determine any changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;

generating an alarm in response to the detection of any such changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;

and using optical communication components to communicate light from the at least one source to more than one of the fibers and to communicate light from more than one of the fibers to the at least one sensor arrangement such that the number of fibers monitored is greater than the number of sources and greater than the number of sensor arrangements;

wherein there is provided a plurality of wavelength division multiplexers (WDMs) such that each monitored fiber has connected thereto at an entry end and an exit end a respective pair of the WDMs for separating the light from the source from a data signal transmitted simultaneously with the monitoring light through the fiber.

10. The method according to claim 9 wherein all transmission on monitored cable is the monitor wavelength of the light source multiplexed to the data wavelength.

11. The method according to claim 9 wherein all loopbacks between WDMs are at the monitor wavelength.

12. A method for detecting movement of optical fibers of an optical fiber cable comprising:

providing a plurality of optical fiber cables arranged in a hub-and-spoke arrangement where each optical fiber cable extends from a main unit at a central location to one of a plurality of remote units;

each optical fiber cable having a first end and a second end, the cable having a plurality of fibers;

monitoring a plurality of fibers of the optical fiber cables by detecting movement of the fibers at locations along the length of the fibers by:

providing at least one source of light at the main unit for injection onto the fibers;

US 7,706,641 B2

9

providing at least one sensor arrangement for receiving light transmitted through the fibers;
 injecting light from the at least one source at the main unit into one end of the each of the fibers to be monitored;
 in the at least one sensor arrangement, detecting a series of received light signals which have been transmitted along the fibers to be monitored;
 in the at least one sensor arrangement, comparing at least some of the received light signals relative to data obtained from previously received ones of the received light signals to detect changes in the received light signals relative to the previously received light signals;
 in the at least one sensor arrangement, analyzing the changes to determine any changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;
 generating an alarm in response to the detection of any such changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;
 and using optical communication components to communicate light from the at least one source at the main unit to more than one of the fibers and to communicate light from more than one of the fibers to the at least one sensor arrangement such that the number of fibers monitored is greater than the number of sources and greater than the number of sensor arrangements
 wherein at least one of the fibers of more than one of the cables is monitored by the light injected into the fibers from said at least one source of light at the main unit.

13. A method for detecting movement of optical fibers comprising:
 providing at least one source of light for injection onto the fibers;
 providing at least one sensor arrangement for receiving light transmitted through the fibers;
 injecting light from the at least one source into one end of each of the fibers to be monitored;

10

in the at least one sensor arrangement, detecting a series of received light signals which have been transmitted along the fibers;
 in the at least one sensor arrangement, comparing at least some of the received light signals relative to data obtained from previously received ones of the received light signals to detect changes in the received light signals relative to the previously received light signals;
 in the at least one sensor arrangement, analyzing the changes to determine any changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;
 generating an alarm in response to the detection of any such changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;
 and using optical communication components to communicate light from the at least one source to more than one of the fibers and to communicate light from more than one of the fibers to the at least one sensor arrangement such that the number of fibers monitored is greater than the number of sources and greater than the number of sensor arrangements;
 wherein there is provided a plurality of optical switches each arranged at a respective end of a respective fiber to be monitored.

14. The method according to claim **13** wherein the optical switches are arranged to break the circuit of a pair of fibers in the event that a movement is detected.

15. The method according to claim **13** wherein the optical switches are arranged to redirect the monitor wavelength round a fiber pair, thereby bypassing a broken link.

16. The method according to claim **13** wherein the optical switches are arranged to scan fibers to identify which one has been intruded, precluding the need for locating.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,706,641 B2
APPLICATION NO. : 11/461917
DATED : April 27, 2010
INVENTOR(S) : Cary R. Murphy et al.

Page 1 of 1

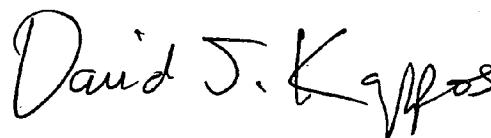
It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title Page Item (75) Inventors should read

Last Name as Giovannini

Signed and Sealed this

Fifteenth Day of June, 2010

A handwritten signature in black ink that reads "David J. Kappos". The signature is written in a cursive, flowing style.

David J. Kappos
Director of the United States Patent and Trademark Office

EXHIBIT 2

INFRINGEMENT CLAIM CHART FOR '641 PATENT

Claim 1 of U.S. Patent No. 7,706,641	CyberSecure System and Method used in PDS System	CyberSecure System and Method used in Data Center Security
1. A method for detecting movement of optical fibers of an optical fiber cable comprising:	CS system monitors optical intrusion and vibration of the fibers. (See Ex. 6)	CS system and method monitors optical intrusion and vibration of the fibers. (See Exs. 4, 5 and 7)
providing a optical fiber cable having a first end and a second end, the cable having a plurality of fibers each of which extends from the first end to the second end;	The PDS system at the DMV Facility includes air blown fibers that extend through a cable comprising one or more microducts (tubes).	The cables at the Primary Customer data centers have a first and second ends and each cable has a plurality of fibers
monitoring a plurality of fibers of the cable by detecting movement of the fiber at locations along the length of the fiber by:	The CS system at the DMV Facility provides for monitoring of the fibers by detecting movement of the fiber at locations along the length of the fiber (e.g., vibration, See Ex. 6)	The CS system and method in use at Primary Customer data centers includes IMS software and an OptiGuard or other Vanguard alternative device that monitors movement of a plurality of fibers and cables. For example, for trunk cables at the data centers, more than one fiber of the cable is monitored.
providing at least one source of light for injection onto the fibers;	The CS system at the DMV Facility includes an OptiGuard or other Interceptor alternative device for providing the source of light injected into the fibers being monitored	The CS system and method in use at Primary Customer data centers includes an OptiGuard or other Vanguard alternative device that includes a light source for injecting the light onto the fibers.
providing at least one sensor arrangement for receiving light transmitted through the fibers;	The CS system at the DMV Facility includes an OptiGuard or other Interceptor alternative device for receiving the light	The CS system and method in use at the Primary Customer data centers includes an OptiGuard or other Vanguard alternative device

	transmitted into the fibers being monitored	for receiving light transmitted through the fibers.
injecting light from the at least one source into one end of each of the fibers to be monitored;	The CS system at the DMV Facility includes an OptiGuard or other Interceptor alternative device for injecting light into one end of the fibers being monitored	The CS system and method at use at Primary Customer data centers includes an OptiGuard or other Vanguard alternative device for injecting the light onto the fibers being monitored
in the at least one sensor arrangement, detecting a series of received light signals which have been transmitted along the fibers to be monitored;	The CS system at the DMV Facility includes an OptiGuard or other Interceptor alternative device for detecting the light signals which have been transmitted along the fibers being monitored	The CS system and method in use at Primary Customer data centers includes an OptiGuard or other Vanguard alternative device for receiving light transmitted along the fibers being monitored
in the at least one sensor arrangement, comparing at least some of the received light signals relative to data obtained from previously received ones of the received light signals to detect changes in the received light signals relative to the previously received light signals;	In the CS system and method in use at the DMV Facility, the system compares at least some of the received light signals relative to data obtained from previously received light signals to detect changes	In the CS system and method in use at the Primary Customer data centers, the system compares at least some of the received light signals relative to data obtained from previously received light signals to detect changes
in the at least one sensor arrangement, analyzing the changes to determine any changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;	In the CS system and method in use at the DMV Facility, the system analyzes the changes in the light signals to determine if the changes are indicative of manipulation causing movement of the optical fiber	In the CS system and method in use at the Primary Customer data centers, the system analyzes the changes in the light signals to determine if the changes are indicative of manipulation causing movement of the optical fiber

generating an alarm in response to the detection of any such changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;	In the CS system and method in use at the DMV Facility, the system generates an alarm when movement of the fiber is detected	In the CS system and method in use at the Primary Customer data centers, the system generates an alarm when movement of the fiber is detected
and using optical communication components to communicate light from the at least one source to more than one of the fibers of the optical fiber cable and to communicate light from more than one of the fibers of the optical fiber cable to the at least one sensor arrangement such that the number of fibers of the optical fiber cable monitored is greater than the number of sources and greater than the number of sensor arrangements.	In the CS system and method in use in the DMV Facility, there are at least two fibers in the air blown fiber cable carrying light from the OptiGuard or other Interceptor alternative device. As a result, there are at least two fibers being monitored which is greater than the single light source present in the OptiGuard or other Interceptor alternative device and is greater than the number of sensor arrangements (e.g., the OptiGuard or other Interceptor alternative device).	In the CS system and method in use at the Primary Customer data centers, the cables and fibers are arranged in a point-to-multipoint network layout so that the OptiGuard or other Vanguard alternative device communicates light to more than one of the fibers of the cable (e.g., the trunk cable) and for the OptiGuard or other Vanguard alternative device to receive light from more than one of the fibers. As a result, the number of fibers being monitored is greater than the number of light sources and greater than the number of sensor arrangements (e.g., the OptiGuard or other Vanguard alternative device).

Claim 8 of US Patent No. 7,706,641	CyberSecure Manhole, Lockbox, and FBG Intrusion Detection System and Method
8. A method for detecting movement of optical fibers comprising:	“CyberSecure IPS sensing systems use light to sense position or movement” of optical fibers. (CS Cyber Sensor Installation Guide, Ex. 8). FBG Sensors are activated by displacing or moving the fiber within the sensor.
providing at least one source of light for injection onto the fibers;	“The light source in the CSMPS-10 system Controller emits in the 1550nm band.” (CS Cyber Sensor Installation Guide, Ex. 8). The OptiGuard M series may also be used as a source of light in Manhole, Lockbox and other FBG sensor systems. (See Ex. 4). The “fibers” are the different Fiber Bragg Gratings within each unique sensor.
providing at least one sensor arrangement for receiving light transmitted through the fibers;	“Information from sensors is obtained by connecting them via optical fiber to a Cyber Sensor Controller device.” (CS Cyber Sensor Installation Guide, Ex. 8). The OptiGuard M series can also be used as a source of light in Manhole, Lockbox and other FBG sensor systems. (See Ex. 4). “System layouts are configured with sensors connected in either a full daisy-chain or a split daisy-chain; examples of each are shown in Figure 2 and Figure 3.” (CS Cyber Sensor Installation Guide, Ex. 8). The sensor arrangement includes the Cyber Sensor Controller device which receives the light transmitted through the fibers. The FBG Controller receives reflections back from sensor fibers.

injecting light from the at least one source into one end of each of the fibers to be monitored;	The light from the CS Controller is injected into the fibers to be monitored. The fiber sensors are daisy-chained along the optical path. The OptiGuard M series can also be used as a source of light in Manhole, Lockbox and other FBG sensor systems. (See Ex. 4).
in the at least one sensor arrangement, detecting a series of received light signals which have been transmitted along the fibers;	The Controller receives the light signals from the sensors. “The Controller polls all sensors in real time and converts optical information from each sensor into position information for that sensor.” (CS Cyber Sensor Installation Guide, Ex. 8). The OptiGuard M series can also be used as a source of light in Manhole, Lockbox and other FBG sensor systems. (See Ex. 4).
in the at least one sensor arrangement, comparing at least some of the received light signals relative to data obtained from previously received ones of the received light signals to detect changes in the received light signals relative to the previously received light signals;	A CyberSecure IPS CSMPS-10 system continuously monitors the location of the manhole sensor and immediately reports a change at any sensor. The OptiGuard M series can also be used as a source of light in Manhole, Lockbox and other FBG sensor systems. (See Ex. 4).
in the at least one sensor arrangement, analyzing the changes to determine any changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;	A CyberSecure IPS CSMPS-10 system continuously monitors the location of the manhole sensors and immediately reports a change at any sensor. Movement of fibers within sensors causes a wavelength change as the detection mechanism. The OptiGuard M series can also be used as a source of light in Manhole, Lockbox and other FBG sensor systems. (See Ex. 4).

generating an alarm in response to the detection of any such changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;	“The CyberSecure CSS™ hardware controller monitors thousands of CyberSecure CSS sensors and is managed by CyberSecure IMS™ (Infrastructure Monitoring System). CyberSecure IMS™ automates intrusion alarm dispatching.” (CyberSecure CSS, Ex. 4). “CyberSecure IMS™ offers comprehensive monitoring of all manholes and handholes with integrated geospatial mapping technology, pinpoint location detection of alarmed manholes, real-time alarm notification via phone, text, email and seamlessly integrates into customizable site specific alarm response and inspection procedures.” (CyberSecure CSS, Ex. 4). The OptiGuard M series can also be used as a source of light in Manhole, Lockbox and other FBG sensor systems. (See Ex. 4).
and using optical communication components to communicate light from the at least one source to more than one of the fibers and to communicate light from more than one of the fibers to the at least one sensor arrangement such that the number of fibers monitored is greater than the number of sources and greater than the number of sensor arrangements;	“In a full daisy-chain configuration, one pigtail on the first sensor connects to one CyberSecure CSS™ Controller channel via SMF-28 optical fiber, and the other pigtail on the first sensor connects (via SMF-28 fiber) to the second sensor on that channel; the second sensor connects to the third sensor on that channel, and so on up to a maximum quantity of 35 sensors on that channel. This is repeated for each of the other CyberSecure CSS™ Controller channels as required.” (CyberSecure CSS, Ex. 4). The OptiGuard M series can also be used as a source of light in Manhole, Lockbox and other FBG sensor systems. (See Ex. 4). “System layouts are configured with sensors connected in either a full daisy-chain or a split daisy-chain; examples of each are shown in Figure 2 and Figure 3.” (CS Cyber Sensor Installation Guide, Ex. 8). Fig. 2:

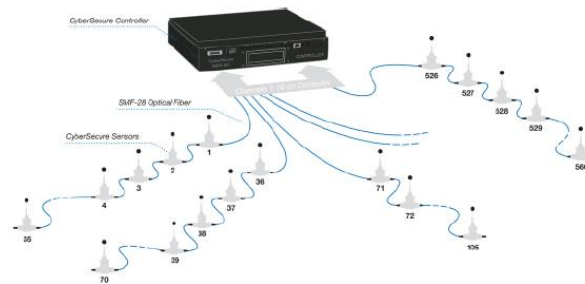
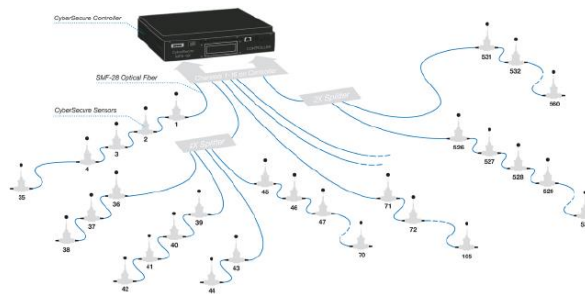


Fig. 3:



wherein the at least one sensing arrangement includes a locating arrangement for detecting the location of a detected movement and wherein there is provided a stored table of fiber lengths of the plurality of fibers which allows the at least one sensing arrangement to determine which fiber of the plurality of fibers has moved.

CyberSecure IMST™ offers comprehensive monitoring of all manholes and handholes with integrated geospatial mapping technology, pinpoint location detection of alarmed manholes. (CyberSecure CSS, Ex. 4).

The OptiGuard M series can also be used as a source of light in Manhole, Lockbox and other FBG sensor systems. (See Ex. 4).

During installation, installers must ensure the wavelength of each sensor matches the intended location in the predefined layout. If a sensor is damaged and must be replaced, then a replacement CSMPS-10 with the same part number (matching wavelength) must be used in that location. The “stored table of fiber lengths” corresponds to the length of the fiber

	between the Bragg periodic structures located within each of the Cyber Sensors.
--	---

Claim 12 of US Patent No. 7,706,641	CyberSecure System and Method used in PDS System	CyberSecure System and Method used in Data Center Security
12. A method for detecting movement of optical fibers of an optical fiber cable comprising:	CS system and method monitors optical intrusion and vibration of the fibers in the cable. (See Ex. 6) The PDS system at the DMV Facility includes air blown fibers that extend through a cable comprising one or more microducts (tubes).	CS system and method monitors optical intrusion and vibration of the fibers. (See Exs. 4, 5 and 7)
providing a plurality of optical fiber cables arranged in a hub-and-spoke arrangement where each optical fiber cable extends from a main unit at a central location to one of a plurality of remote units;	The layout of optical fiber cables in the PDS at the DMV Facility is a point to multipoint layout which corresponds to a hub-and-spoke arrangement that includes a main unit (e.g., an OptiGuard or other alternative Vanguard device) and a remote unit (e.g., a concatenation or Remote Termination Unit).	The layout of optical fiber cables at the Primary Customer data centers is a point to multipoint layout which corresponds to a hub-and-spoke arrangement that includes a main unit (e.g., an OptiGuard or other alternative Vanguard device) and a remote unit (e.g., a concatenation or Remote Termination Unit).
each optical fiber cable having a first end and a second end, the cable having a plurality of fibers;	The cables in the PDS at the DMV Facility have first and second ends and the cables include air blown fibers.	The cables at the Primary Customer data centers have first and second ends and each of the cables has a plurality of fibers

monitoring a plurality of fibers of the optical fiber cables by detecting movement of the fibers at locations along the length of the fibers by:	The CS system and method in use at the DMV Facility provides for monitoring of the fibers by detecting movement of the fiber at locations along the length of the fiber (e.g., vibration, See Ex. 6)	The CS system and method in use at Primary Customer data centers includes IMS software and an OptiGuard or other Vanguard alternative device that monitors movement of a plurality of fibers and cables
providing at least one source of light at the main unit for injection onto the fibers;	The CS system and method in use at the DMV Facility includes an OptiGuard or other Interceptor alternative device for providing the source of light injected into the fibers being monitored	The CS system and method in use at Primary Customer data centers includes an OptiGuard or other Vanguard alternative device that includes a light source for injecting the light onto the fibers.
providing at least one sensor arrangement for receiving light transmitted through the fibers;	The CS system and method in use at the DMV Facility includes an OptiGuard or other Interceptor alternative device for receiving the light transmitted into the fibers	The CS system and method in use at the Primary Customer data centers includes an OptiGuard or other Vanguard alternative device for receiving light transmitted through the fibers.
injecting light from the at least one source at the main unit into one end of the each of the fibers to be monitored;	The CS system and method in use at the DMV Facility includes an OptiGuard or other Interceptor alternative device for injecting light into one end of the fibers being monitored	The CS system and method in use at Primary Customer data centers includes an OptiGuard or other Vanguard alternative device for injecting the light into one end of the fibers being monitored
in the at least one sensor arrangement, detecting a series of received light signals which have been transmitted along the fibers to be monitored;	The CS system and method in use at the DMV Facility includes an OptiGuard or other Interceptor alternative device for detecting the light signals which have been transmitted along the fibers being monitored	The CS system and method in use at Primary Customer data centers includes an OptiGuard or other Vanguard alternative device for receiving light transmitted along the fibers being monitored

in the at least one sensor arrangement, comparing at least some of the received light signals relative to data obtained from previously received ones of the received light signals to detect changes in the received light signals relative to the previously received light signals;	In the CS system and method at the DMV Facility, the system compares at least some of the received light signals relative to data obtained from previously received light signals to detect changes	In the CS system and method in use at the Primary Customer data centers, the system compares at least some of the received light signals relative to data obtained from previously received light signals to detect changes
in the at least one sensor arrangement, analyzing the changes to determine any changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;	In the CS system and method in use at the DMV Facility, the system analyzes the changes in the light signals to determine if the changes are indicative of manipulation causing movement of the optical fiber	In the CS system and method in use at the Primary Customer data centers, the system analyzes the changes in the light signals to determine if the changes are indicative of manipulation of the optical fiber
generating an alarm in response to the detection of any such changes which are indicative of manipulation of the optical fiber causing movement of a portion thereof along the length thereof;	In the CS system at the DMV Facility, the system generates an alarm when movement of the fiber is detected	In the CS system and method in use at the Primary Customer data centers, the system generates an alarm when movement of the fiber is detected
and using optical communication components to communicate light from the at least one source at the main unit to more than one of the fibers and to communicate light from more than one of the fibers to the at least one sensor arrangement such that the number of fibers monitored is greater than the	In the CS system and method in use in the PDS at the DMV Facility, the cables and fibers are arranged in a point-to-multipoint network layout so that the OptiGuard or other Interceptor alternative device communicates light to more than one of fibers and the OptiGuard or other Interceptor alternative device receives light from more than one of the fibers. As a	In the CS system and method in use at the Primary Customer data centers, the cables and fibers are arranged in a point-to-multipoint network layout so that the OptiGuard or other Vanguard alternative device communicates light to more than one of the fibers and the OptiGuard or other Vanguard alternative device receives light from more than one of the fibers. As a

number of sources and greater than the number of sensor arrangements	result, the number of fibers being monitored is greater than the number of light sources and greater than the number of sensor arrangements (e.g., IMS software and OptiGuard or other Interceptor alternative device).	result, the number of fibers being monitored is greater than the number of light sources and greater than the number of sensor arrangements (e.g., IMS software and OptiGuard or other Vanguard alternative device).
wherein at least one of the fibers of more than one of the cables is monitored by the light injected into the fibers from said at least one source of light at the main unit.	In the CS system and method in use in the PDS at the DMV Facility, at least one fiber of more than one cable is monitored by injecting light from the OptiGuard or other Interceptor alternative device.	In the CS system and method in use at the Primary Customer data centers, at least one fiber of more than one cable is monitored by injecting light from the OptiGuard or other Vanguard alternative device.

EXHIBIT 3

INTERCEPT™ & INTERCEPT™ CS Optical Network Security System



INTERCEPT™



INTERCEPT™ CS

The INTERCEPT™ monitors two or more dark (spare, unused) fibers within a cable carrying classified information. INTERCEPT supports standard single-mode and multimode fiber optic cables and can be used to secure existing network infrastructure. Using patented hub and spoke technology, a single INTERCEPT utilizing one rack space can monitor up to eight continuous optical circuits (zones), providing protection for multiple remote buildings or many dozens of user drops per zone in a facility. When dark data fibers are not available, INTERCEPT+Plus can be used to monitor active fibers. A Remote Termination Unit (RTU) is required for each zone when using the INTERCEPT+Plus. Contact us for more details.

INTERCEPT™ CS is a bundled solution consisting of the INTERCEPT and CyberSecure Infrastructure Management System, a software application that provides NIS monitoring devices with the capability to centrally manage alarms, create PDS Standard Operating Procedures (SOPs), eliminate false alarms and automatically guide user responses to alarms and more.

Generic Specifications for INTERCEPT & INTERCEPT CS

Electrical

Power Input 100/240V, 250mA 60/50Hz IEC
C14 3-Position Connector

Environmental

Operating Temperature 0°C - 45°C
Storage Temperature -10°C - 50°C
Operating Humidity 20% - 80% Non-Condensing

Physical

1U high, 19" Rack Mountable
H x W x D: 45 x 432 x 368 mm
H x W x D: 1.75 x 17.0 x 14.5 inches

Weight

6.4 kg (14 lbs)

Local Management

Channel LED indicators, Channel Reset Buttons

Remote Management

RS232 Serial: Console Access
TACACS+ Compatible
10/100BaseT Ethernet: SSHv2, Telnet,
SNMPv2c, SNMPv3
INTERCEPT CS has a 1000BASE-T Ethernet connection

Alarm Management

SNMPv2c, SNMPv3, Syslog,
Self-Test Heartbeat LED Indicator
Email, SMS alerts
NO/NC Contacts
INTERCEPT CS incorporates a Unidirectional
Simplex Optical Communications Port for sending
alarms to an optional Cross-Domain Communications Unit

Optional Features

Rear connections
Connector types other than SC-UPC
Aerial fiber monitoring
Active fiber monitoring

Optical

1, 2, 4 or 8 Ports (multimode)
1, 2 or 4 Ports (single-mode)
SC UPC Non-Angled Duplex Connectors
Dynamic range: 1, 2, or 4 port multimode 50dB
Dynamic range: 8 port multimode 20dB
Dynamic range: single-mode 55dB
Note: Designed for 3dB Excess/Safety
Lead-in fiber multimode: Sensitive or Desensitized
Lead-in fiber single-mode: Sensitive

Industry Certifications & Features

The INTERCEPT is UL, FCC Part 15, IEC Class 1,
CDRH Class I, and CE rated & certified

*For specifications on all other products and extended
warranty and support plans, please refer to our website
at www.networkintegritysystems.com*

VANGUARD™ and VANGUARD™ CS

Fiber Optic Monitoring System



VANGUARD™ CS

VANGUARD™ INTRODUCTION

The VANGUARD™ Fiber Optic Network Monitoring System uses patented technologies to ensure the integrity and availability of network data by monitoring two or more dark (spare, unused) fibers within the optical cables making up the infrastructure. This 24/7/365 monitoring immediately detects and reports tampering or intrusion attempts conducted for the purposes of data theft (tapping) or denial of service. VANGUARD is used on standard single-mode or multimode fiber, and with Plug-and-Protect™ capability, VANGUARD can rapidly be added to new or existing network infrastructure.

Using patented hub and spoke technology, a single VANGUARD™ utilizing one rack space can monitor up to eight continuous optical circuits (zones), providing protection for multiple remote buildings or many dozens of user drops per zone in a facility. When dark data fibers are not available, VANGUARD+Plus can be used to monitor active fibers. A Remote Termination Unit (RTU) is required for each zone when using the VANGUARD+Plus.

VANGUARD™ Standard Features

- VANGUARD is available in 1, 2, 4 and 8 (multimode only) channel platforms
- RS-232 serial port for system configuration
- 10/100/1000Base-T connector for remote configuration and alarm reporting
- Relay alarm contact closures for monitoring and equipment alarm notification
- Auto-configure feature available to automatically set alarm thresholds
- Alarm parameters adjustable via serial port or Ethernet connection
- Dual redundant power supply

VANGUARD™ CS

The VANGUARD™ CS is a bundled solution consisting of the VANGUARD™ and CyberSecure Infrastructure Management System, a software application that provides VANGUARD with the capability to centrally manage alarms, create PDS Standard Operating Procedures (SOPs), set alarm thresholds to eliminate nuisance alarms and automatically guide user responses to alarms and more.

VANGUARD™ CS Hardware Differences

Note: Except for those listed below, all features of a standard VANGUARD™ are still present in the VANGUARD™ CS version.

1. VANGUARD CS front panel Ethernet port operates at up to 1000Base-T gigabit Ethernet
2. VANGUARD CS includes a rear panel simplex ST optical port for connection to the optional VANGUARD CS-Cross Domain Communications Unit (XDU). See our website or contact us for additional information on the XDU.

VANGUARD™ and VANGUARD™ CS

Fiber Optic Monitoring System

VANGUARD™ Technical Specifications

Electrical

Power Input	100/240V, 60/50Hz, Max. Current approx. 250mA IEC, 3 position power connector (IEC C14)
Battery (Controller Board)	Duracell: CR2032 Lithium-Manganese Dioxide (Not field replaceable ~ At Factory Only)

Environmental

Operating Temperature	0°C - 45°C
Storage Temperature	-10°C - 50°C
Operating Humidity	20% - 80% Non-Condensing

Physical

Dimensions	1U high, 19" Rack Mountable HxWxD 4.5 x 43.2 x 36.8 cm (1.75 x 17.0 x 14.5 inches)
------------	--

Weight

6.4 kg (14 lbs)

Ports

Console	DB-9 male
Ethernet	RJ-45 female
Alarm Contacts	Normally open or Normally closed – equipment alarm, global monitoring alarm and channel monitoring alarm 30 Vdc 0.5A maximum

System Management

Remote Management	SSH v2, Telnet, SNMP via 10/100/1000Base T Ethernet, and RS232 serial. 1000Base T to be used with shielded Cat6 cable Maximum 2 concurrent user interface sessions Maximum 1 concurrent SNMP query
Local Management	Channel LED indicators, Channel reset buttons
Alarm Notification	SNMP, Email, SMS, Relay Alarm Contracts

Optical Specifications

Channel Configuration	1, 2, 4, or 8 (multimode only) Channels
Max. Optical Receiver Input	-7.5 dBm SMF, -12.5 dBm MMF
Shutdown Reaction Time	< 100ms
Optical Connector Type	Either SC or LC duplex- CAUTION: UPC NON-ANGLED
Laser Safety Rating	IEC: Class 1(IEC60825-1 Ed. 2 (2007)) Ed. 3 (2014) CDRH: Class 1 (21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007)

Industry Certifications & Features

The VANGUARD™ is UL, FCC Part 15, IEC Class 1, CDR Class 1, and CE rated & certified Additional International Certifications - Inquire with Factory.

For specifications on all other products and extended warranty and support plans, please refer to our website at www.networkintegritysystems.com

EXHIBIT 4



CYBERSECURE IPS

INFRASTRUCTURE PROTECTION SYSTEM

OPTI-GUARD™ M-Series

Opti-Guard™ M - Series with Flex-Port Technology

CyberSecure IPS is proud to offer the Opti-Guard™ M - Series, the most sophisticated critical infrastructure intrusion detection device available today with the power of Flex-Port technology. The Opti-Guard™ M - Series revolutionizes alarmed fiber intrusion detection hardware technology and is managed by CyberSecure IPS' RMF accredited CyberSecure IMS software.

The modular composition of the M-Series hardware promotes flexibility and scalability to provision any customer environment and use case with ease, utilizing 'Flex-Port' technology. Flex-Port technology reduces cost and complexity, provides extreme adaptability, and future-proofs inside and outside plant critical infrastructure protection for any application. The patented security for real-time threat assessment and situational awareness is available in three versatile models: the M4, M8, and M16.

CyberSecure IPS' end-to-end portfolio offers a true turn-key alarmed fiber critical infrastructure intrusion detection solution to include hardware, software, installation services, training, 5-Year warranty and 24x7x365 technical support to ensure your critical infrastructure is safe and secure.

Opti-Guard™ M-Series Product Highlights

- 4-Port, 8-Port & 16-Port Models
- Flex-Port Technology on ALL Ports
- Cyber-Sensing Arrays for Intrusion Location Detection
- Lock-box / Pull-box Sensor Intrusion Detection
- Manhole Sensor Intrusion Detection
- Data Center Cage Intrusion Detection
- On/Off Ramp Sensors for Lead-In / Lead-Out Alarmed Fibers
- Optical Accelerometer Sensors for Seismic Activity Sensors
- Cable Tray Intrusion Monitoring Sensors
- Up to 30 Sensing Points per Channel with the Cyber Sensing Array
- 25dB Dynamic Sensing Range
- Dual Power Supplies for Redundancy
- Rapid Connect Barcode Enrollment
- No Special Cables Required
- M4 (1RU), M8 (2RU), M16 (2RU)
- Standard 5-year Hardware Warranty

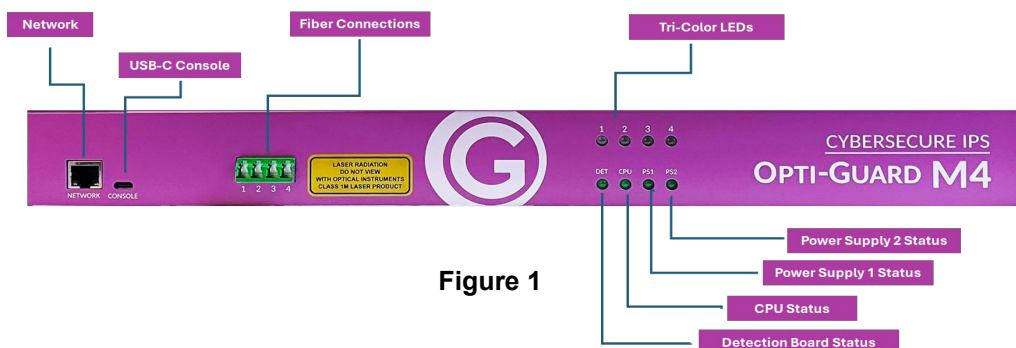


Figure 1

OPTI-GUARD M-SERIES FLEX-PORT DETECTION METHODS

The Opti-Guard™ M-Series expands critical infrastructure intrusion detection methods to include several new monitoring capabilities to help customers protect their critical infrastructure with less equipment, less fiber and more visibility. As shown below in Figure 2, customers can choose which type of monitoring best suits their application on a port by port basis with a single hardware platform.

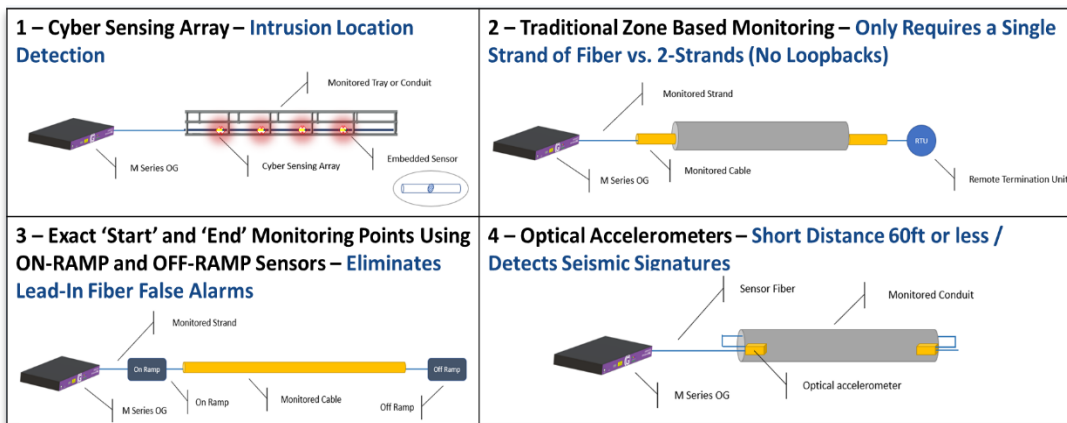


Figure 2

OPTI-GUARD M-SERIES FLEX-PORT TECHNOLOGY: ANY PORT – ALL APPLICATIONS

The most revolutionary technology advancement offered by the Opti-Guard™ M-Series is Flex-Port technology. As shown below in Figure 3, Opti-Guard™ M-Series customers have the ultimate application flexibility by having the ability to purchase a single hardware platform and support numerous infrastructure protection applications.

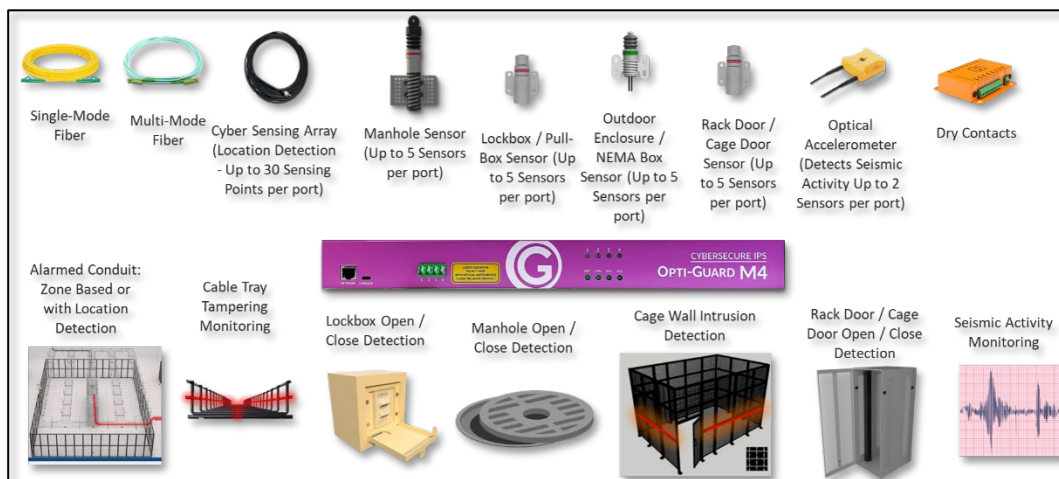


Figure 3

The CyberSecure IPS Opti-Guard M™ Series provides an economic solution for critical infrastructure security monitoring packed in a small footprint. Designed for “out of the box” monitoring and the ultimate application flexibility, the Opti-Guard M series provides will secure your critical infrastructure. Combined with CyberSecure IMS™, the M series can be locally or globally managed and cost effectively supports small, medium and large deployments. Please contact sales@cybersecureips.com for more information.

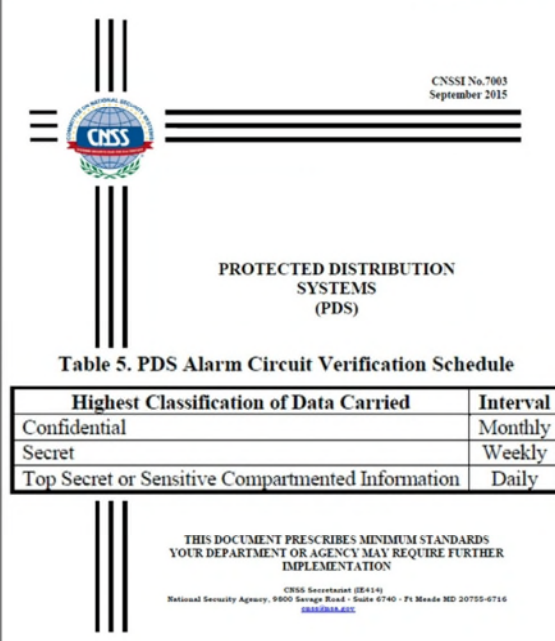
EXHIBIT 5



CYBERSECURE IPS

CYBERSECURE IPS – Compliance & Capabilities

- Integrated CNSSI 7003 compliant SOP
- RMF Accredited on NIPR & SIPR
- Fiber Forensics™ eliminates nuisance and false alarms
- Optical warning thresholds
- Automated alarm circuit verification
- Data shut-off capability
- Information Assurance (IA) Management



CNSSI No. 7003
September 2015

PROTECTED DISTRIBUTION
SYSTEMS
(PDS)

Table 5. PDS Alarm Circuit Verification Schedule

Highest Classification of Data Carried	Interval
Confidential	Monthly
Secret	Weekly
Top Secret or Sensitive Compartmented Information	Daily

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER
IMPLEMENTATION

CNSSI Secretariat (2E414)
National Security Agency, 9800 Savage Road - Suite 6740 - Ft Meade MD 20755-6716
[NSA/SS/2015-010](#)

EMSEC solution – PDS through alarmed fiber. 8 IPS containers can be cut to 1.

**CYBERSECURE IPS**

HARDWARE PRODUCTS – Infrastructure Protection



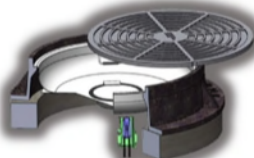
Opti-Guard™ M-Series
Fiber Monitoring



STOPLIGHT™
Automated Testing / Data Shut-Off



Cyber Sensing Array™
Customized Intrusion Locations



LockDown™ Security Device

CYBER SENSORS



Cyber Sensor Controller™
Enclosure Monitoring



Cyber Sensor™
Lockbox Sensor



Maintenance Hole
Sensor

INTEGRATION SUPPORT



USER DESKTOP BOX



CAMERA/VMS



DRY CONTACT

Opti-Guard (OG) is new technology (traditional detection) basically replace the Interceptor alarm cable. Eliminating TACLANES. IA Mgnt. RMF credit for NIPR and SIPR. OSP Stoplight – 1 port for 5 hand hole sensors



CYBERSECURE IPS

CyberSecure IMS

Outside Plant Protection

Underground Perimeter Protection

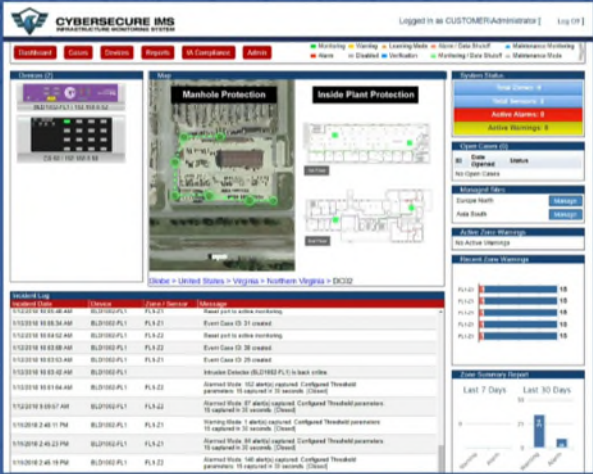
OSP Utility Pathway Protection

Zero Power Manhole Sensors

OSP Fiber Pathway Protection

Fiber Damage / Dig Detection

Centralized Management Global Architecture



CyberSecure
Infrastructure Monitoring System (IMS)

Inside Plant Protection

ISP / Secure Conduit

Perimeter Cage Sensor

Cage Door

Rack Door Sensor

Floor Monitoring

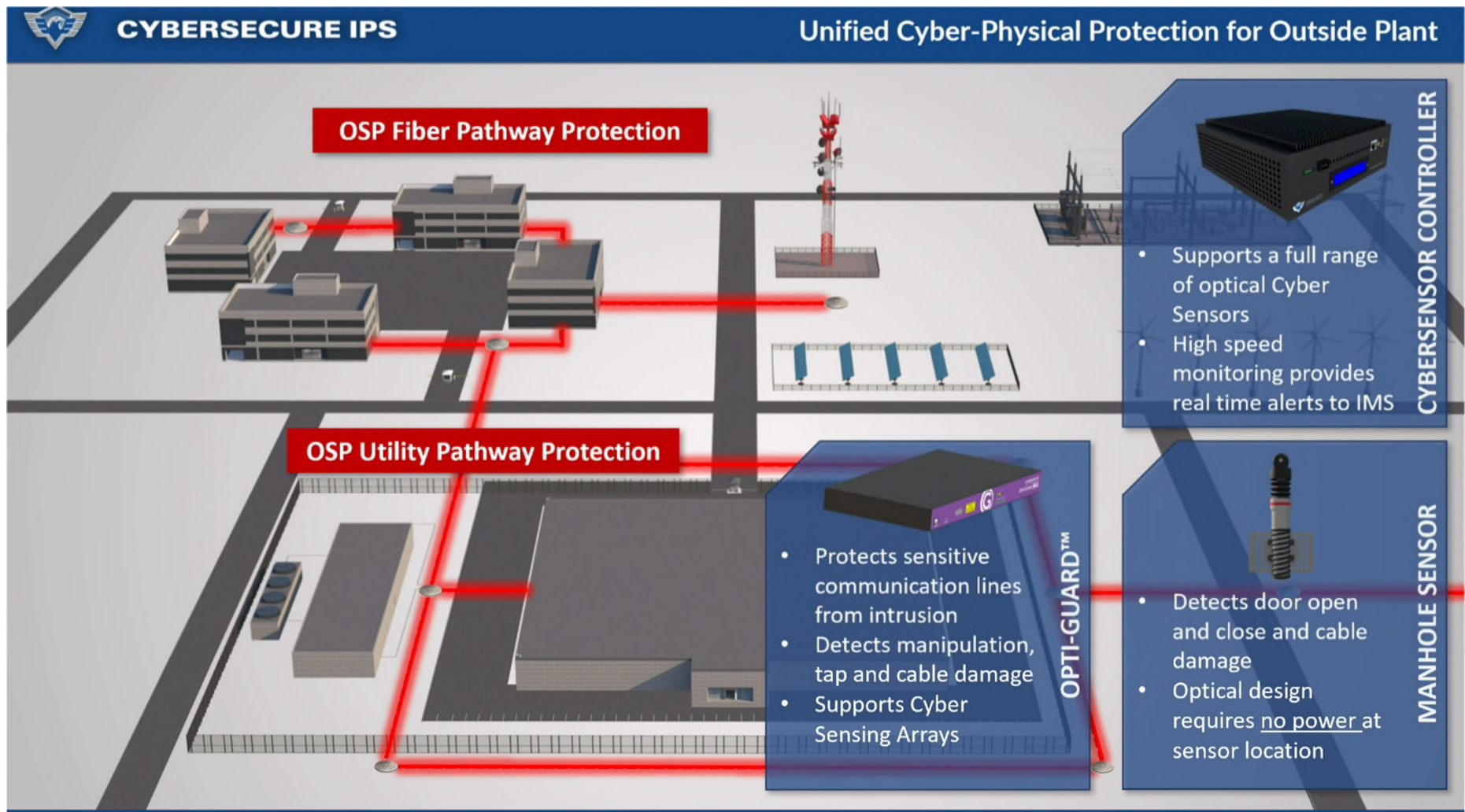
Lockbox Sensor

CyberTag™ RFID

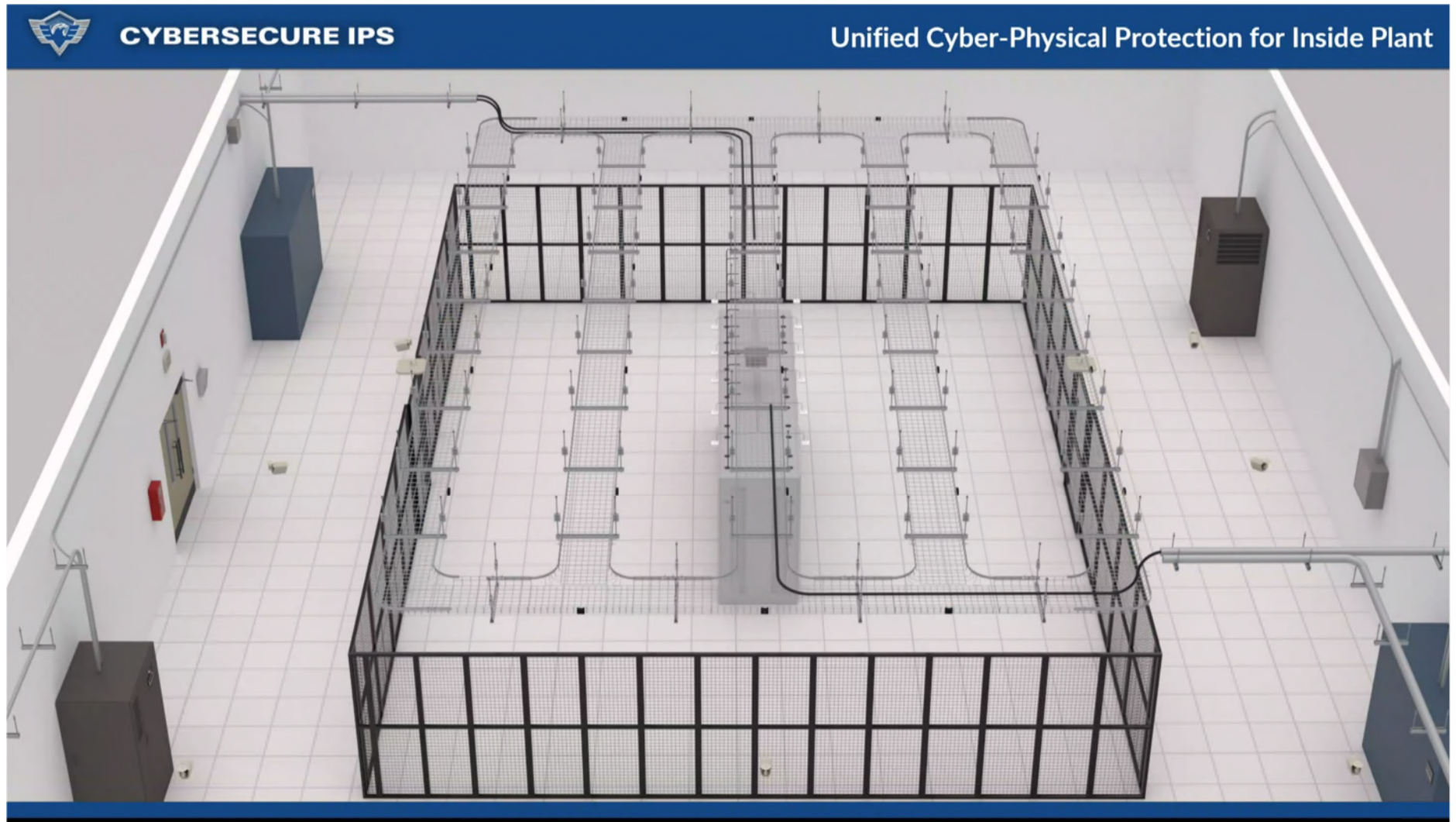
Camera Integration

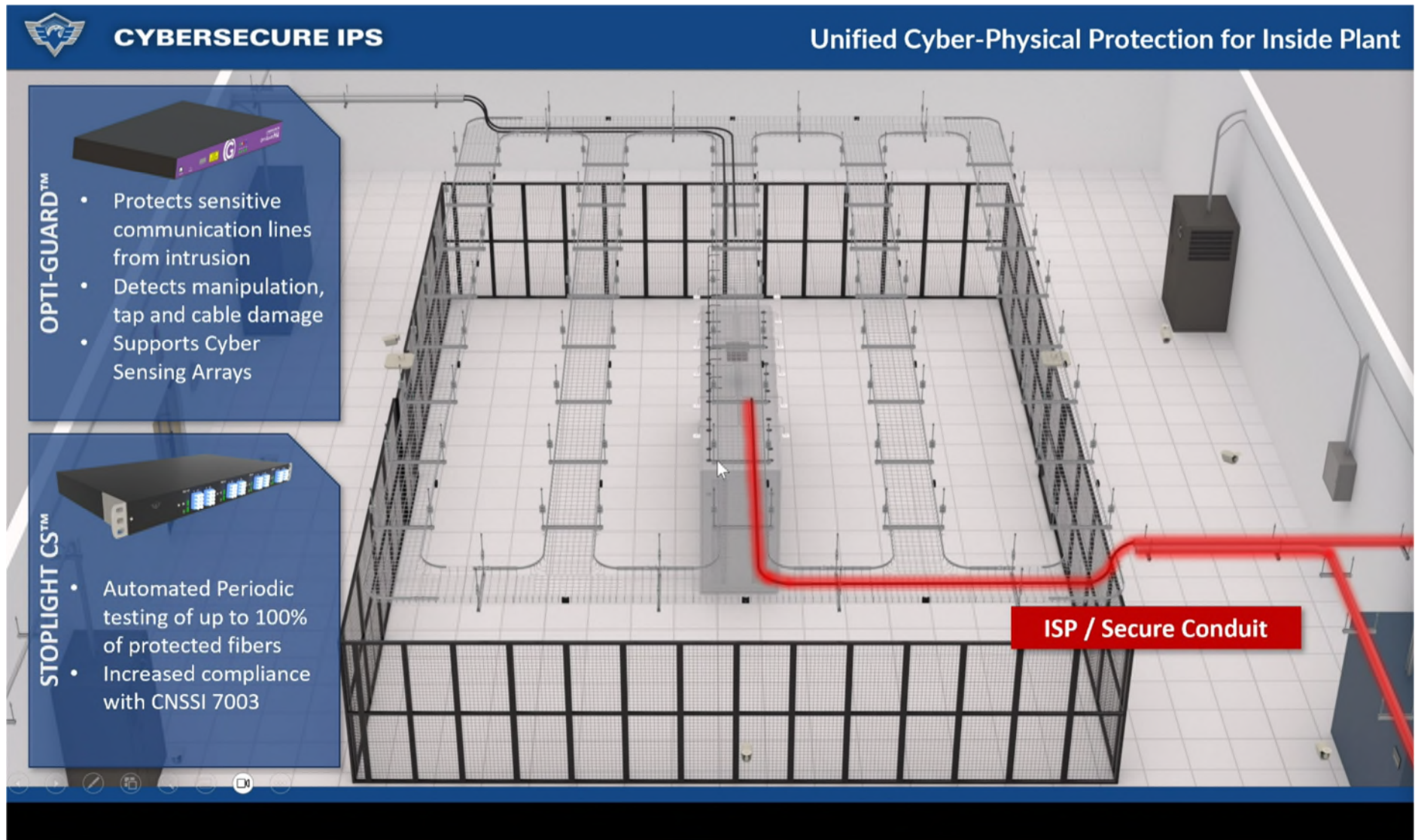


Unified Cyber-Physical Protection (UCP) for Outside Plant Protection



Single mode – no power – dark fiber – alarming hand holes. IMS Management System located? Who monitors? Monitor hand hole alarms. CCRI failure fixes





Stoplight sold with OG for Inside Plant monitoring.

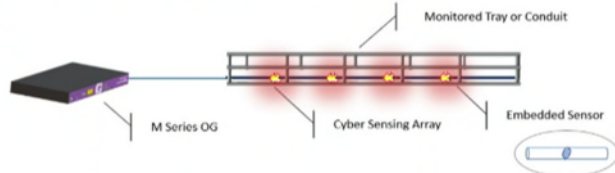


CYBERSECURE IPS

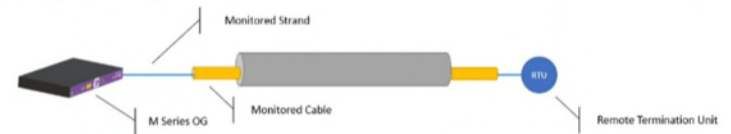
FLEX-PORT TECHNOLOGY DETECTION METHODS

OPTI-GUARD™ M-SERIES FLEX PORT DETECTION METHODS

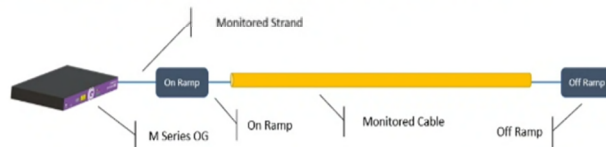
1 CYBER SENSING ARRAY Intrusion Location Detection



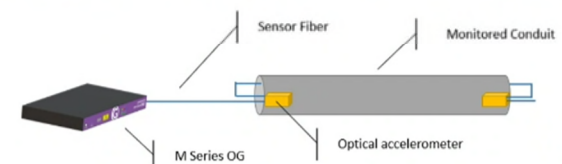
3 TRADITIONAL ZONE BASED MONITORING Only Requires a Single Strand of Fiber vs. 2-Strands (No Loopbacks)



2 EXACT 'START' AND 'END' MONITORING POINTS USING ON-RAMP AND OFF-RAMP SENSORS Eliminates Lead-In Fiber False Alarms



4 OPTICAL ACCELEROMETERS Short Distance 60ft or less / Detects Seismic Signatures





CYBERSECURE IPS

OPTI-GUARD™ M-SERIES FLEX-PORT TECHNOLOGY: Any Port – All Applications



Single-Mode
Fiber



Multi-Mode
Fiber



Cyber Sensing Array
(Location Detection -
Up to 30 Sensing
Points per port)



Manhole Sensor
(Up to 5 Sensors
per port)



Lockbox / Pull-
Box Sensor (Up
to 5 Sensors
per port)



Outdoor
Enclosure /
NEMA Box
Sensor (Up to 5
Sensors per port)



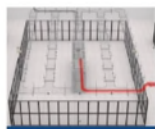
Rack Door /
Cage Door
Sensor (Up
to 5 Sensors
per port)



Optical
Accelerometer
(Detects Seismic
Activity Up to 2
Sensors per port)



Dry
Contacts



Alarmed Conduit:
Zone Based or with
Location Detection



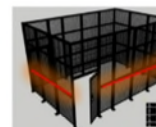
Cable Tray
Tampering
Monitoring



Lockbox Open /
Close Detection



Manhole Open /
Close Detection



Cage Wall
Intrusion
Detection



Rack Door / Cage
Door Open / Close
Detection



Seismic
Activity
Monitoring



CYBERSECURE IPS

STOPLIGHT™ - INTEGRATE WITH OPTI-GUARD™ FOR COMPLETE COMPLIANCE

STOPLIGHT™

- Automated alarm circuit verification, up to 100% of Alarmed PDS Fibers
- Disables data by stopping the light
- 100% Cyber Operational Readiness Assessment (CORA) pass rate when total UCP System implemented (Software & Hardware)





CYBERSECURE IPS

Unified Cyber-Physical Protection

CYBERSECURE IMS

CENTRALIZED MANAGEMENT

CyberSecure Infrastructure Monitoring System (IMS) is a web-based monitoring system that provides customers:

- Real time notifications, warnings and alarms
- Intrusion Forensics
- Event Case Management
- Dispatching and Notification

It is a Microsoft Windows based solution, installed on customer provided infrastructure and allows users across the Enterprise to access monitoring and detection information



**CYBERSECURE IPS**

Unified Cyber-Physical Protection

CYBERSECURE IMS**CENTRALIZED MANAGEMENT**

Patented Protection for real time threat assessment and situational awareness.

NOTIFICATION	3 RD PARTY INTEGRATION	AUTHENTICATION	PROTOCOLS
• SMTP • SNMP • Dry Contact Relay System (ADAM, Fargo) • Syslog	• Molex • Pelco • RLS • Inner Range • Vindicator • Tellabs • PON/SPON • ExacqVision	• Active Directory • LDAP • OpenID Connect (OIDC) • AWS Federate • TACACS	• RTSP • SNMP • REST • SSH • WebSocket • GraphQL • Custom Protocol /Raw Socket



CYBERSECURE IPS

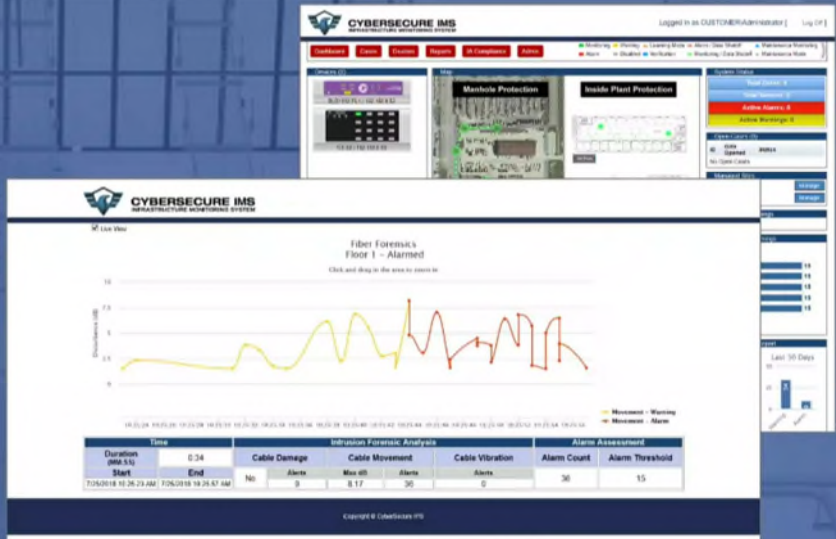
Unified Cyber-Physical Protection

CYBERSECURE IMS

OPTICAL **WARNING** THRESHOLD FIBER FORENSICS™

Patented Protection for real time threat assessment and situational awareness.

Graphical representation of every optical disturbance as it occurs, personnel can use this information to determine immediate and appropriate alarm response including on-site inspection.



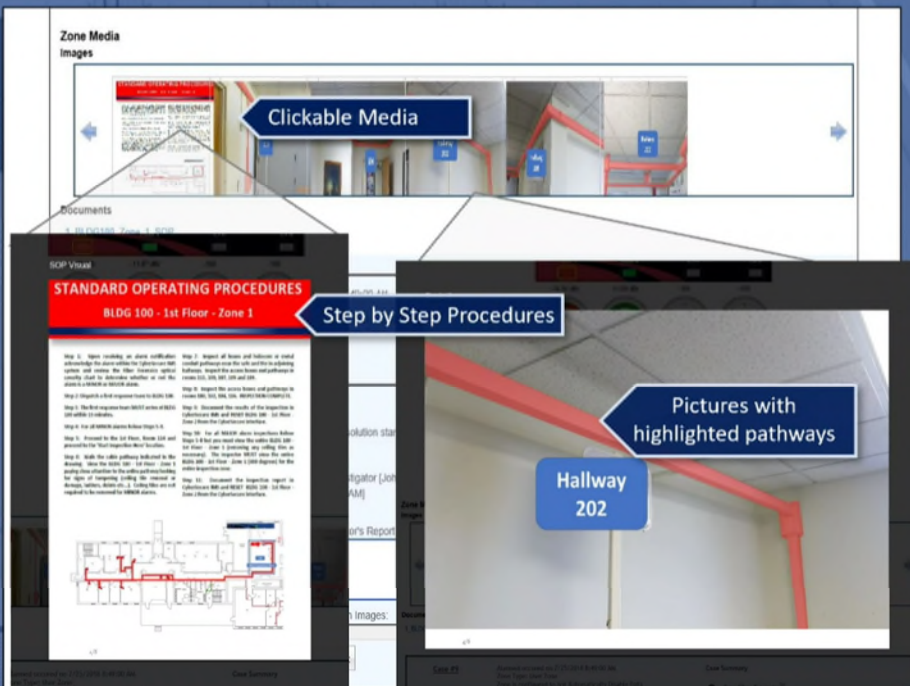

CYBERSECURE IPS

Unified Cyber-Physical Protection

CYBERSECURE IMS

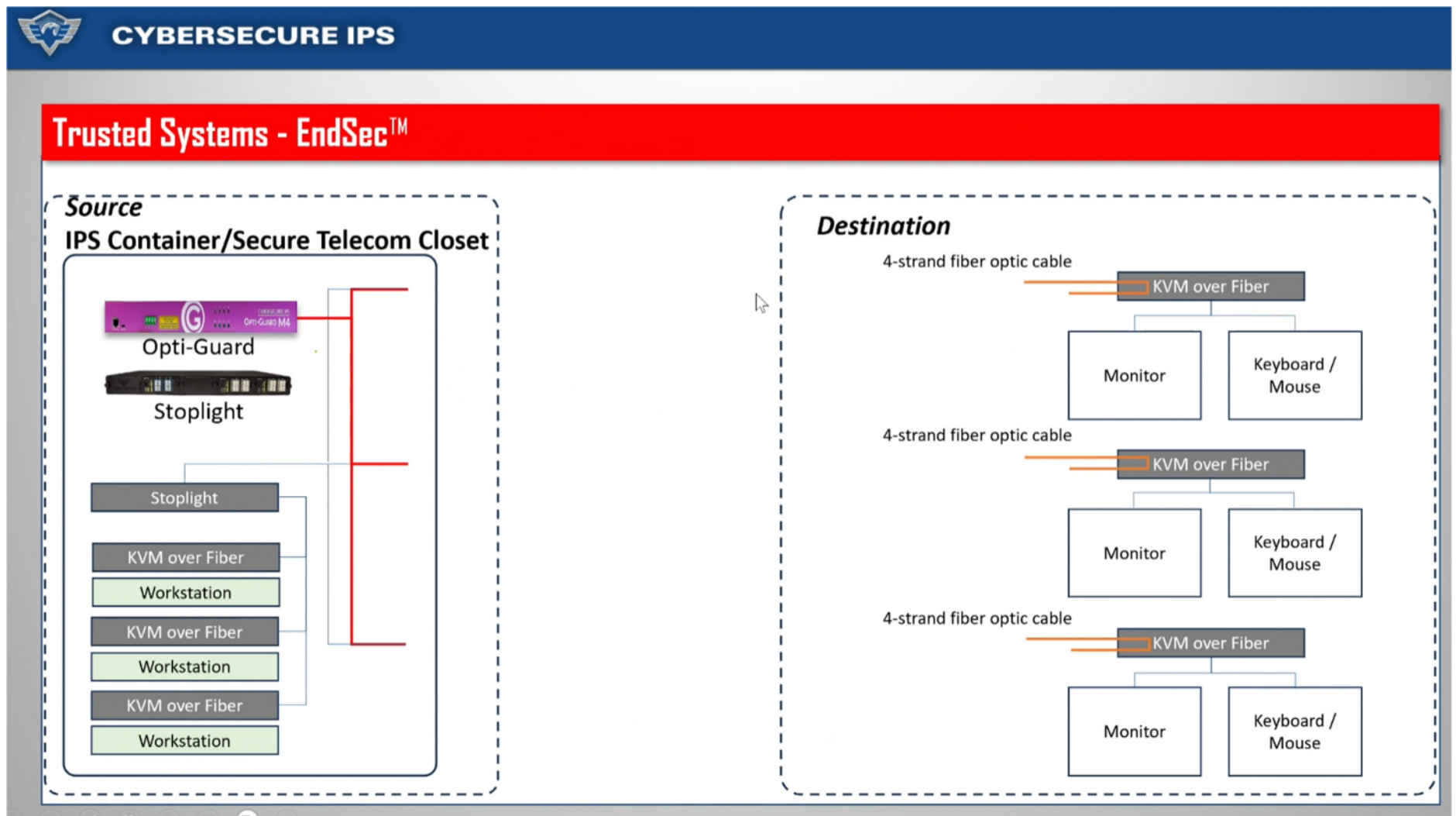
INTEGRATED SOP

Case management with integrated SOPs and automated reports.



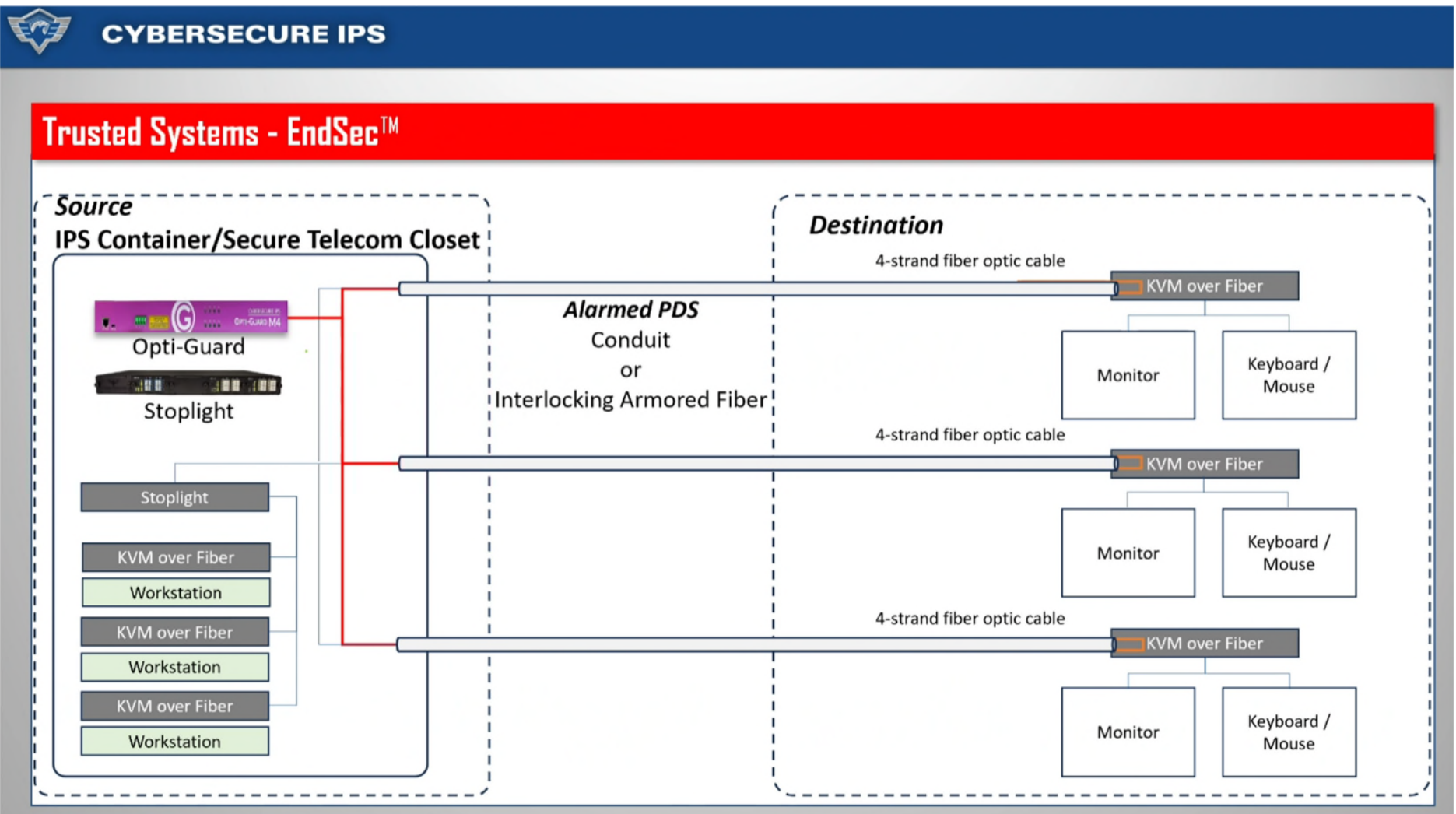
The interface displays a central 'Zone Media Images' section with a 'Clickable Media' button. Below this is a 'Documents' section titled 'STANDARD OPERATING PROCEDURES BLDG 100 - 1st Floor - Zone 1'. To the right, a 'Step by Step Procedures' section is visible. At the bottom right, a 'Pictures with highlighted pathways' section shows a hallway labeled 'Hallway 202' with red lines indicating movement paths.





4sm fiber (2) – Alarm (2) – KVM 8 containers on our original quote could be cut to 1 container SIPR VDI??

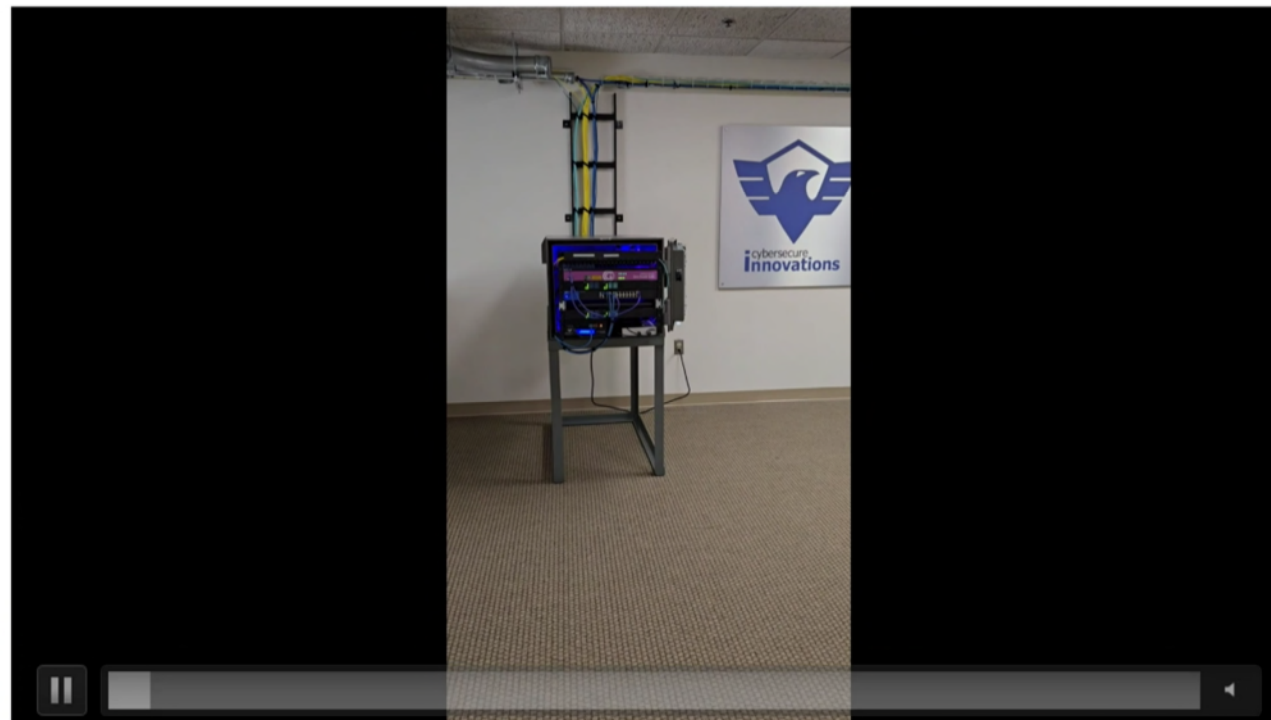
Anya Kasischke anya@trustedsys.com (410)756-3300 Jason Aguilar jason.aguilar@cybersecureips.com (719) 659-6048

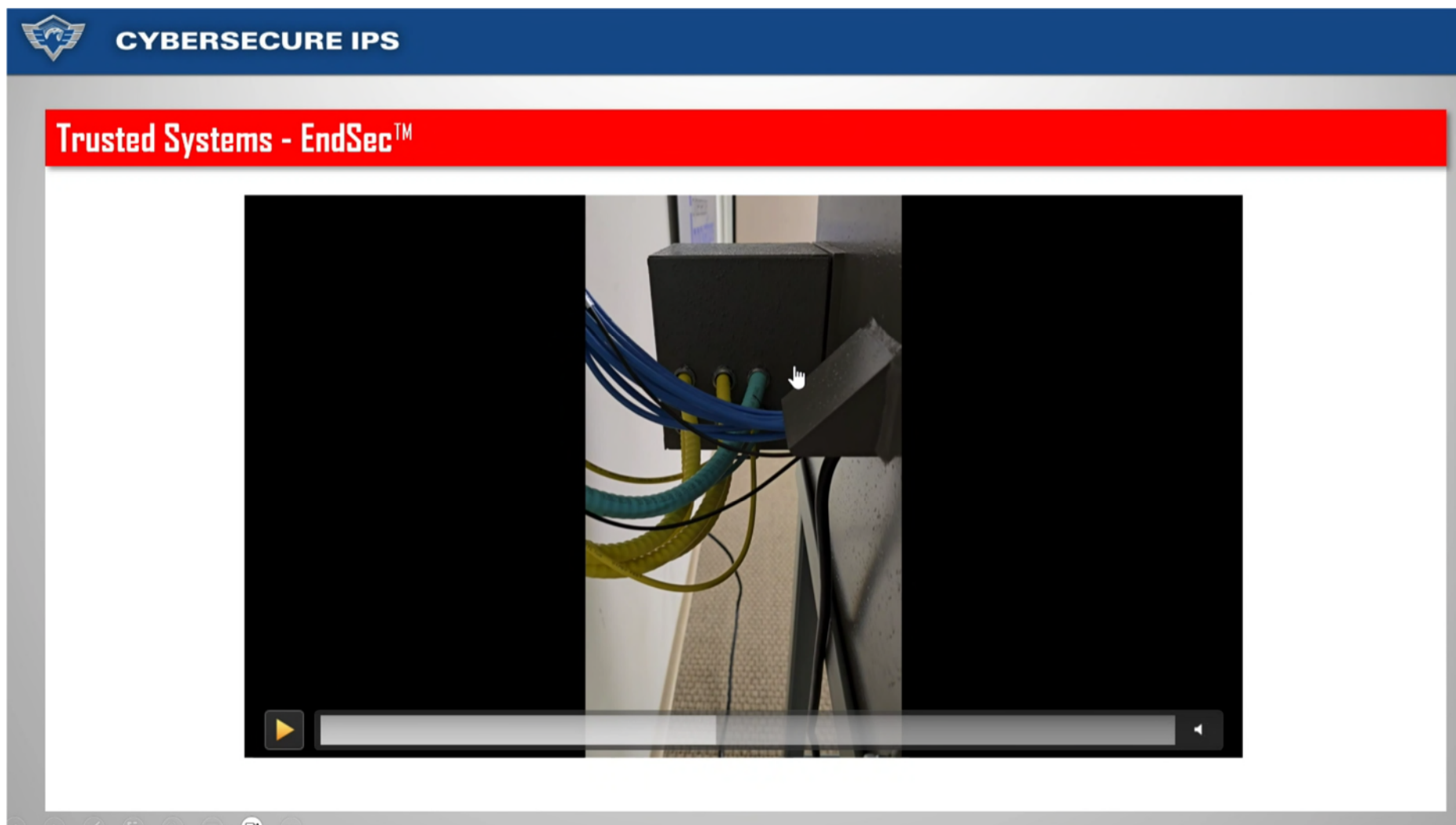




CYBERSECURE IPS

Trusted Systems - EndSec™

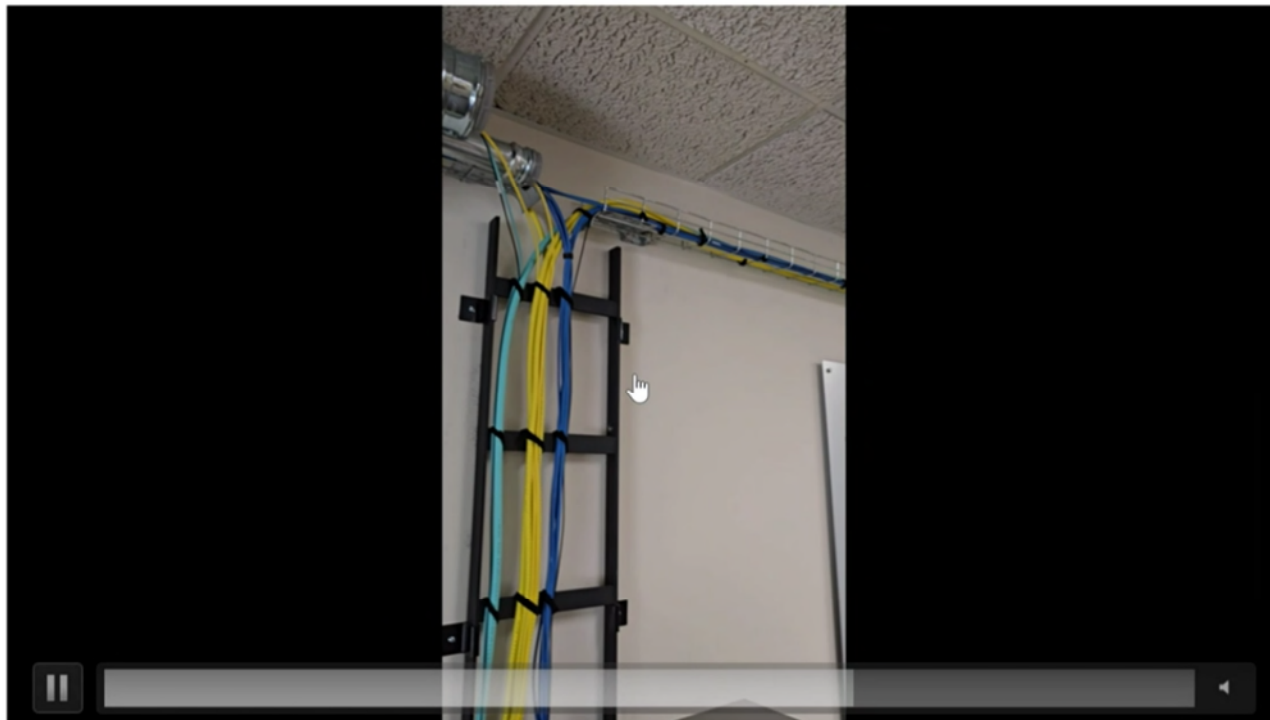






CYBERSECURE IPS

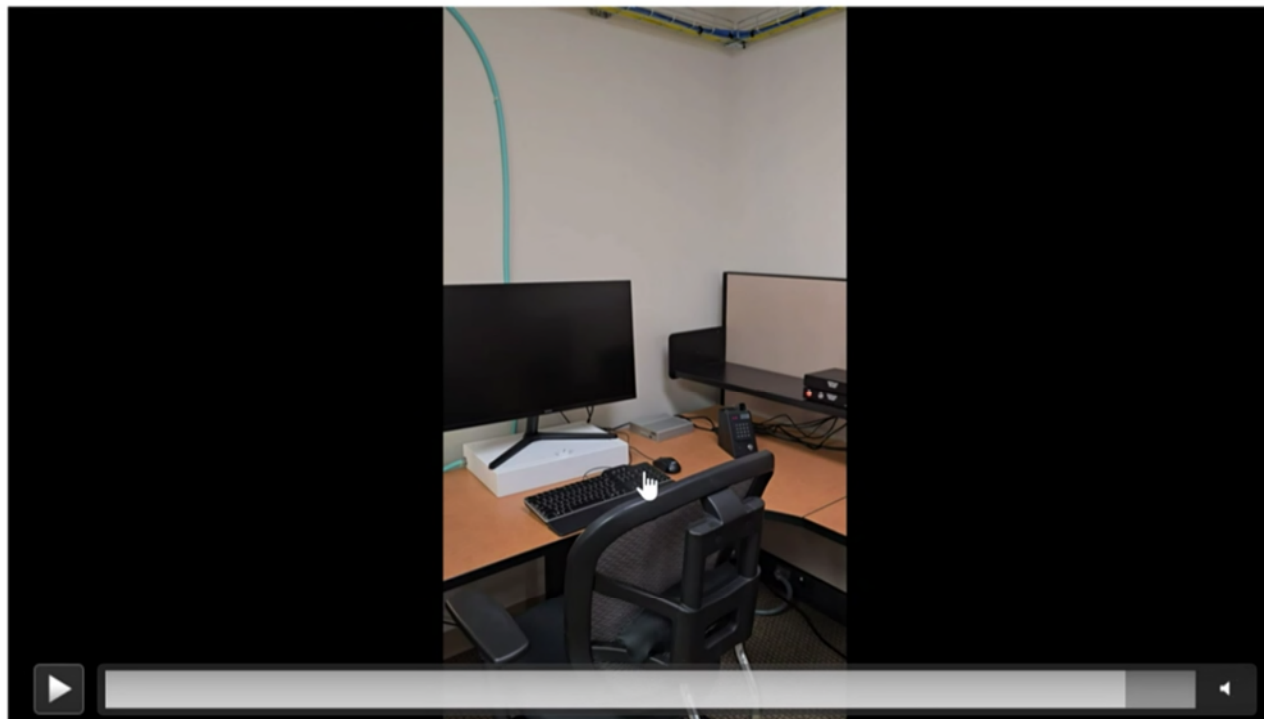
Trusted Systems - EndSec™





CYBERSECURE IPS

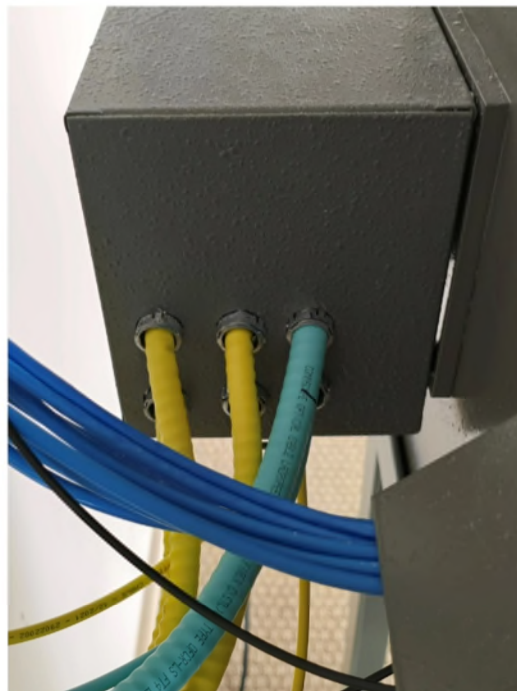
Trusted Systems - EndSec™





CYBERSECURE IPS

Trusted Systems - EndSec™



Training

Design – Provide floor plans – # of workstations and locations marked on floor plans (controlled/non-controlled areas)

License/Support Constraints

SOW/IGE/Work Plan

GSA not recommended. Other vehicles other than local CONS available

Langley Tech Lead – SOW available

EXHIBIT 6

COMMERCIAL SOLUTIONS

REALIZE TRUE DATA CENTER SECURITY WITH CYBERSECURE IPS

IS YOUR NETWORK INFRASTRUCTURE SAFE WHEN YOU ARE NOT THERE?

Colocation services offer great growth and scalability opportunities. However, trusting your data to a third-party landlord who doesn't monitor infrastructure can be a huge risk. With open cages, unprotected meeting rooms, and no remote surveillance, all it can take to bring down your entire network is an intruder plugging in a single USB drive.

GET MORE INFORMATION ([HTTPS://WWW.CYBERSECUREIPS.COM/GET-MORE-INFORMATION-COMMERCIAL-SOLUTIONS/](https://www.cybersecureips.com/get-more-information-commercial-solutions/))

TOTAL VISIBILITY OF YOUR ENTIRE FACILITY - FROM CAGES TO ASSETS

Protect your network by installing powerful, yet discrete unified cyber-physical protection that delivers real-time in-depth situational awareness. Our best-of-breed sensors detect even the slightest disturbances and provide continuous surveillance that you can access anytime, anywhere, in a single dashboard.

INSIDE AND OUTSIDE PHYSICAL THREATS ARE TODAY'S HEADWINDS

The whole world is watching. It seems like every day another Fortune 500 company makes the headlines for failing to keep data safe. Enterprises are under more pressure than ever before to protect their networks – especially from their own employees and 3rd party partners, among all other outside threats that are growing recently.

\$8.7 MILLION

**THE AVERAGE COST OF
INSIDER ATTACKS**

ARE YOU SEEING THE BIG PICTURE OF SECURITY?

It's time for CIOs and CISOs to work together. With the widespread adoption of IoT and IIoT devices, we've entered into a new era of hybrid attacks that blur the lines between physical and cybersecurity. Our solution, built from the feedback of Fortune 500 NOC/SOC teams, integrates your entire operation.

DIVIDE AND BE CONQUERED

No matter the type of threat, all enterprises face the same security problems. Siloing security teams results in unclear communication, lack of visibility, and a hindered ability to identify and respond to complex threats.

BRING IT ALL TOGETHER WITH THE CYBERSECURE IPS SOFTWARE SOLUTION

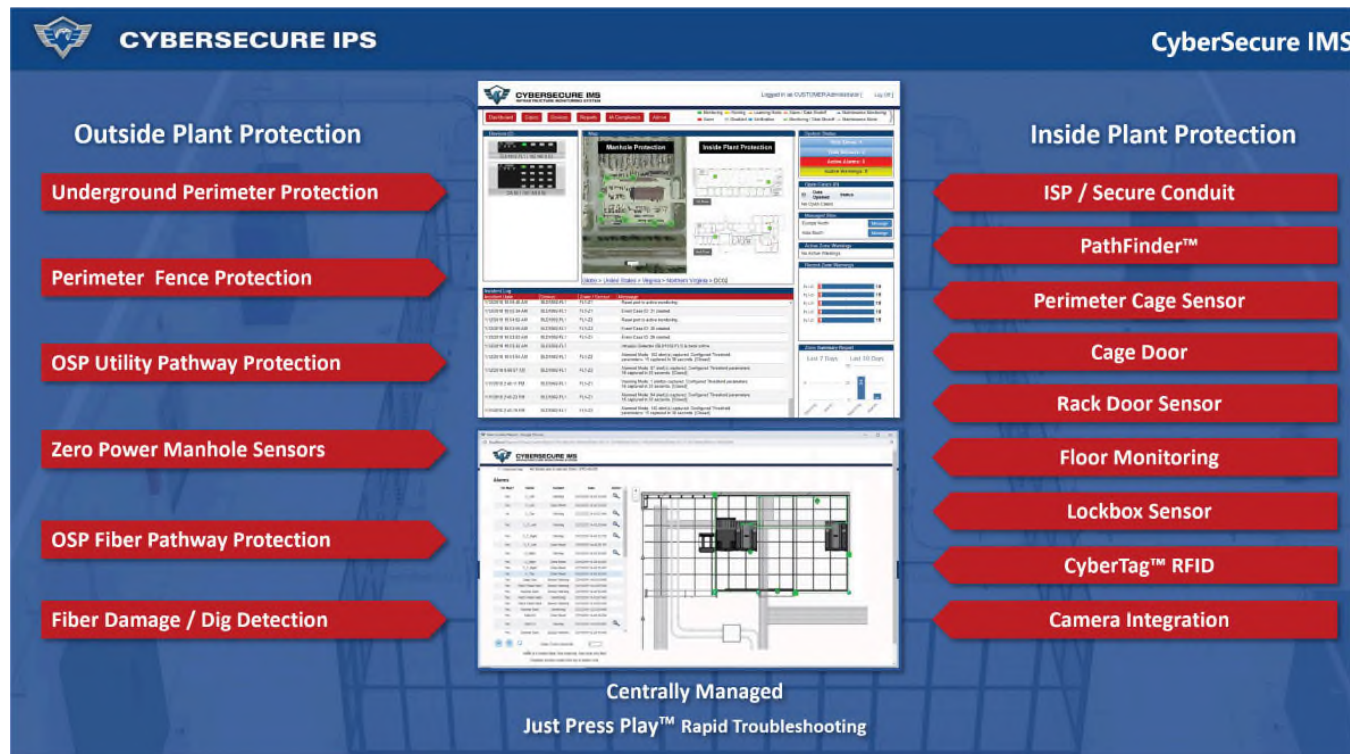
Groundbreaking features included with our Infrastructure Monitoring System (IMS) software allow you to monitor, analyze, and manage data from various protection systems in a single real-time dashboard.

OUR DATA CENTER PROTECTION SUITE

The solution is unified cyber-physical protection. We monitor all pathways and assets with pioneering sensors that feed into our Infrastructure Monitoring System, providing you with a clear picture of your organization in a single pane of glass. Work with our experts to design the set of features perfect to suit your organization.



MULTIPLE LAYERS OF PROTECTION:



Our data center security suite protects and monitors all aspects of your network infrastructure in a unified solution. This includes all areas inside your facility and all grounds and pathways outside and around your facility.

PERIMETER FENCES
MAINTENANCE HOLES
OSP PATHWAYS AND CONDUITS

UTILITY PATHWAYS
RAISED FLOOR
CAGE PERIMETERS
CAGE DOOR

LADDER RACK
CABINET DOOR
ISP PATHWAYS & CONDUITS

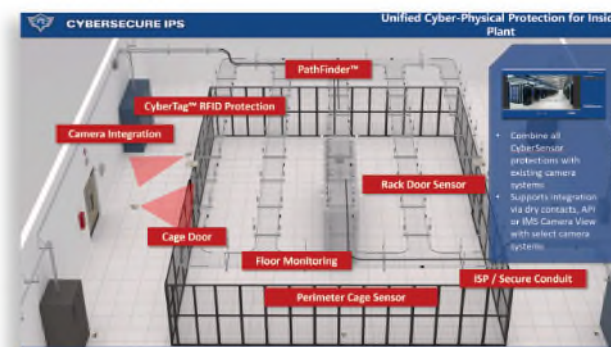


OUTSIDE PLANT PROTECTION

Watch over the entire outside perimeter of your facility and way beyond. Our patented hardware and sensors allow you to monitor perimeter grounds, utility pathways, fiber pathways, and manhole access points. With precise, location-specific feedback data all types of threats and interferences outside can be detected and eliminated quickly.

INSIDE PLANT PROTECTION

From floor sensors and cage sensors to cable pathways and assets, our inside facility security solutions offer 100% complete coverage of your data center. Our inside plant security also monitors areas typically left unchecked like data halls, "Meet Me" rooms, demarcation points, and distribution points.



AN EASY INVESTMENT

Our Data Center Protection Suite streamlines security operations to deliver peace of mind. It can be retro-fitted into existing infrastructure to minimize installation effort and cost. Plus, it scales with you, growing into global environments as your organization expands.

READY TO PROTECT AND DEFEND YOUR NETWORK?

GET IN TOUCH WITH US TO DISCUSS A CUSTOM SECURITY SOLUTION.

GET IN TOUCH WITH US ([HTTPS://WWW.CYBERSECUREIPS.COM/GET-MORE-
INFORMATION-COMMERCIAL-SOLUTIONS/](https://www.cybersecureips.com/get-more-information-commercial-solutions/))



3 Bethesda Metro Center
Suite 700
Bethesda, MD 20814
1 (844) 653-1018

International: 1-240-696-1311
Fax: 1-301-760-3906

UCP
([HTTPS://WWW.CYBERSECUREIPS.COM/LEARN-MORE-UCP/](https://www.cybersecureips.com/learn-more-ucp/))

DUNS # 079096912 - CAGE # 6ZRP5

COMMERCIAL
([HTTPS://WWW.CYBERSECUREIPS.COM/COMMERCIAL-SOLUTIONS/](https://www.cybersecureips.com/commercial-solutions/))

Alarmed Carrier PDS | CNSSI 7003, AR 25-2

Compliant | Authority to Operate (ATO) | Risk
Management Framework (RMF)

GOVERNMENT
([HTTPS://WWW.CYBERSECUREIPS.COM/GOVERNMENT-SOLUTIONS/](https://www.cybersecureips.com/government-solutions/))

PRODUCTS
([HTTPS://WWW.CYBERSECUREIPS.COM/OUR-PRODUCTS/](https://www.cybersecureips.com/our-products/))

ABOUT
([HTTPS://WWW.CYBERSECUREIPS.COM/ABOUT-US/](https://www.cybersecureips.com/about-us/))

NEWS
([HTTPS://WWW.CYBERSECUREIPS.COM/NEWS/](https://www.cybersecureips.com/news/))

BLOG
([HTTPS://WWW.CYBERSECUREIPS.COM/BLOG/](https://www.cybersecureips.com/blog/))

CONTACT
([HTTPS://WWW.CYBERSECUREIPS.COM/CONTACT-US/](https://www.cybersecureips.com/contact-us/))

© 2025 CyberSecure IPS | All Rights Reserved

EXHIBIT 7

GOVERNMENT SOLUTIONS

ALARMED CARRIER PDS SOLUTIONS FOR MILITARY AND GOVERNMENT

SECURE CLASSIFIED NETWORKS AND ENSURE 100% COMPLIANCE IS MET EVERY TIME

Government organizations that must comply with CCSNI 7003 can meet these strict and challenging security standards much easier with our Alarmed Carrier PDS solutions. Manage and automate the laborious and costly visual inspections and testing required for CCSNI 7003 compliance.

GET MORE INFO ([HTTPS://WWW.CYBERSECUREIPS.COM/GET-MORE-INFORMATION-GOVERNMENT-MILITARY-SOLUTIONS/](https://www.cybersecureips.com/get-more-information-government-military-solutions/))

CENTRALLY MONITOR THREATS, AUTOMATE INSPECTIONS & RESPONSE PROCEDURES

Our Centrally Managed Alarmed Carrier PDS System is a combination of best of breed hardware and software solutions that provide uninterrupted surveillance, smart analysis, and automated responses to any disturbance. It collects and displays real-time monitoring statistics based on the severity and duration of all potential intrusion attempts.



COMMON CHALLENGES WITH PROTECTED DISTRIBUTION SYSTEMS (PDS)

These are the challenges that most military sites face with traditional PDS systems when it comes to inspections and security.

- 1 Rigorous regular inspections require heavy manpower. With government agencies operating on reduced budgets, it's difficult to staff during weekends and holidays, not to mention getting a response team to an alarm site within the mandatory 15 minutes during off-hours.
- 2 The phrase "human error" exists for a reason. Manual inspections can result in inaccuracies on inspection forms.
- 3 Most PDS systems use encryption, which slows down their bandwidth and decreases productivity.



SOLVE TRADITIONAL PDS PROBLEMS WITH OUR SCALEABLE SOLUTIONS

By installing continuous surveillance of your classified network infrastructure and automating inspections, you can eliminate errors, ensure all inspections are passed and save on costs over time.

OUR ALARMED CARRIER PDS SOLUTIONS PROVIDE:

REAL-TIME DASHBOARD – ACCESSIBLE REMOTELY

TIME-STAMPED INSPECTION DOCUMENTATION

AUTOMATIC DATA DISABLEMENT TO ALARMED ZONE

OPTICAL WARNING SYSTEM – USER-CONFIGURABLE THRESHOLDS

IMMEDIATE ALARM DISPATCHING



THE TECHNOLOGY BEHIND OUR ALARMED CARRIER PDS SOLUTION

Our hardware, software, and cyber sensor components work together to meet your security challenges and ensure you achieve CNSSI 7003 compliance.



CYBERSECURE IMS™

All information is processed by our Infrastructure Monitoring System, the brain of the solution. IMS keeps time-stamped documentation, generates case files,



alerts the response team, controls data flow to the alarmed zones and sends notifications to all necessary parties.

CYBERSENSOR CONTROLLER™

High-speed monitoring of a full range of optical Cyber Sensors. Support up to 16 channels, each of which supports up to 50 sensors. Provides real-time alerts.



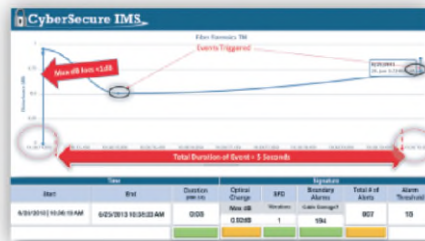
STOPLIGHT™

Fiber optic panel that automatically performs alarm circuit verification required by CNSSI 7003 for any size building. Includes software-controlled ability to disable classified data. Sends out customized reports after each periodic test. Capable of random scheduled testing. Out-of-band and non-intrusive.

FIBER FORENSICS™

CyberSecure's Fiber Forensics™ technology provides alarm response dispatchers with an optical intrusion severity chart to allow the dispatchers to respond according to the severity of the optical intrusion.

The Fiber Forensics chart measures specific metrics that correlate directly to fiber tap techniques to determine the severity of all optical intrusion attempts.



DURATION OF THE OPTICAL INTRUSION (TIME)

THE CHANGE IN LIGHT WITHIN THE ALARMED FIBERS (DB CHANGE)

THE NUMBER OF VIBRATIONS THAT OCCUR DURING AN OPTICAL INTRUSION ATTEMPT

LET US BRING YOU PEACE OF MIND

Our 24/7/365 continuous monitoring immediately detects and reports every disturbance from the slightest bumps to the most sophisticated data theft attempts. We customize our technology to work for you, setting Site-Specific Operating Procedures for every client.

GET IN TOUCH WITH US ([HTTPS://WWW.CYBERSECUREIPS.COM/GET-MORE-
INFORMATION-GOVERNMENT-MILITARY-SOLUTIONS/](https://www.cybersecureips.com/get-more-information-government-military-solutions/))



3 Bethesda Metro Center
Suite 700
Bethesda, MD 20814
1 (844) 653-1018

International: 1-240-696-1311
Fax: 1-301-760-3906

UCP
([HTTPS://WWW.CYBERSECUREIPS.COM/LEARN-
MORE-UCP/](https://www.cybersecureips.com/learn-more-ucp/))

DUNS # 079096912 - CAGE # 6ZRP5

COMMERCIAL
([HTTPS://WWW.CYBERSECUREIPS.COM/COMMERCIAL-
SOLUTIONS/](https://www.cybersecureips.com/commercial-solutions/))

Alarmed Carrier PDS | CNSSI 7003, AR 25-2
Compliant | Authority to Operate (ATO) | Risk
Management Framework (RMF)

GOVERNMENT
([HTTPS://WWW.CYBERSECUREIPS.COM/GOVERNMENT-
SOLUTIONS/](https://www.cybersecureips.com/government-solutions/))

PRODUCTS
([HTTPS://WWW.CYBERSECUREIPS.COM/OUR-
PRODUCTS/](https://www.cybersecureips.com/our-products/))

ABOUT
([HTTPS://WWW.CYBERSECUREIPS.COM/ABOUT-
US/](https://www.cybersecureips.com/about-us/))

NEWS
([HTTPS://WWW.CYBERSECUREIPS.COM/NEWS/](https://www.cybersecureips.com/news/))

BLOG
([HTTPS://WWW.CYBERSECUREIPS.COM/BLOG/](https://www.cybersecureips.com/blog/))

CONTACT
([HTTPS://WWW.CYBERSECUREIPS.COM/CONTACT-
US/](https://www.cybersecureips.com/contact-us/))

EXHIBIT 8



CYBERSECURE IPS

INFRASTRUCTURE PROTECTION SYSTEM

Cyber Sensor Installation Guide

EX-2005

Page 92

CyberSecure IPS...Securing Data from Within

CyberSecure IPS is the world's first U.S. Government certified secure interactive infrastructure monitoring application designed specifically to DETECT, PROTECT and SECURE government and commercial network critical infrastructures.

CyberSecure IPS gives network managers the ability to monitor and protect the physical security of their critical network infrastructures. CyberSecure IPS simplifies information assurance (IA) management, creates and manages site-specific compliant standard operating procedures and generates a unique case resolution audit trail. CyberSecure IPS provides robust protection against critical infrastructure intrusion attempts and dispatches the appropriate first response teams in real-time.





CYBERSECURE IPS

INFRASTRUCTURE PROTECTION SYSTEM



Installation Guide for Cyber Sensor – CSMPS-10 Manhole Cover Position Monitoring System

Table of Contents

Introduction.....	4
Principle of Operation	4
Figure 1: CSMPS-10 manhole cover position sensor	4
Preconditions.....	5
Figure 2: Full daisy-chain configuration	5
Figure 3: Split daisy-chain configuration options	5
Loss Factors and Maximum Allowable Losses	6
Table 1: Summary of maximum allowable losses	6
Sensor Installation	7
Figure 4: Manhole profiles and CSMPS-10 sensor placements	7
Figure 5: Vertical Wall	7
Figure 6: Protective mounting hardware and adjustable bracket	7
Cyber Sensor Controller.....	8
Figure 8: Cyber Sensor Controller	8
Table 2: CSMPS-10 part numbers.....	8
Appendix A	9
Stripping of polyimide coating from optical fiber	9
Mechanical Stripping	9
Chemical Stripping	9
Thermal Stripping	10
Splicing Equipment.....	10
Appendix B	11
Equipment for testing integrity of optical fiber and splices, and measuring power.....	11
Contact Us.....	11



1. Introduction

Note:

This document describes general installation procedures for CSMPS-10 manhole cover monitoring systems. The details of mounting hardware and methods will inevitably vary depending on the configuration of the manholes being monitored. Installers should consult the separate installation configuration drawings that define and detail the specific hardware and methods to use in a given system.

CSMPS-10 manhole cover position sensing systems are specifically designed to help protect the security of communication system infrastructures by monitoring manholes that provide access to underground communication lines and components. CSMPS-10 systems are part of the CyberSecure IPS suite of fiber optic sensing systems made by CyberSecure IPS. CyberSecure IPS sensing systems use light to sense position or movement. CyberSecure IPS sensors contain no electronic components, require no electrical power and radiate no signals. An CSMPS-10 system for manhole cover monitoring consists of CSMPS-10 sensors, Cyber Sensor Controller monitoring equipment at a remote location, optical fiber that connects the sensors with the monitoring equipment, and user interface software. A CyberSecure IPS CSMPS-10 system continuously monitors the position of manhole covers and immediately reports a change at any cover. Hundreds of covers may be monitored simultaneously if desired, and every cover is individually identified. Individual identification allows exact location of any attempt to access underground utility or communication systems through a manhole on which a sensor has been installed, and facilitates an immediate focused response by security or law enforcement personnel if appropriate.

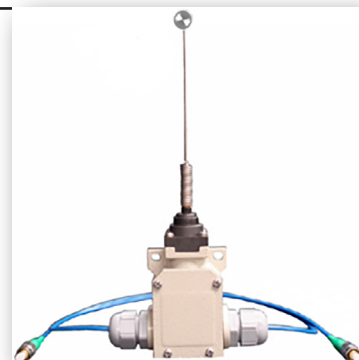
2. Principle of Operation

An CSMPS-10 sensor package consists of a sealed, environmentally rugged housing that contains a fiber optic sensing element known as a fiber Bragg grating (FBG), a toggle mechanism, ruggedized optical fibers that extend through seals on the sides of the housing, and a stainless steel actuator stem that extends from the top of the housing and operates the internal toggle. A representative sensor is shown in Figure 1. Information from sensors is obtained by connecting them via optical fiber to a Cyber Sensor Controller device. The Controller polls all sensors in real time and converts optical information from each sensor into position information for that sensor. The Cyber Sensor Controller 1, 4, 8 and 16 parallel channels.

Those CSMPS-10 sensors connected to any single Controller channel are configured so each has a unique address, thus avoiding any potential ambiguity in identification of any individual sensor. With proper system configuration, each Controller channel will support up to 50 sensors, so a 16-Channel Cyber Sensor Controller can simultaneously poll up to 800 manhole covers. If more than 800 manholes are to be monitored, additional Controllers may be used, each monitoring an additional increment of up to 800 sensors.

Figure 1

CSMPS-10 manhole cover position sensor



Cyber Sensor Installation Guide

3. Preconditions

All CSMPS-10 sensors are delivered with two pre-installed optical fiber pigtails having a standard length of 3 meters. Light travels through the sensor in either direction, so the pigtails are interchangeable for installation purposes. The pigtails must be fusion spliced into SMF-28 single-mode optical fiber, which in turn either terminates at the Cyber Sensor Controller or leads to other CSMPS-10 sensors. Splicing and checkout prior to operation must be performed using appropriate equipment. See Appendix A for information on stripping techniques required for polyimide-coated fiber. See Appendix B for information on system checkout equipment and techniques.

To achieve reliable performance with 50 sensors per channel, CyberSecure IPS strongly recommends meeting the following preconditions:

- 1.** Sensors are connected in wavelength order, starting with the shortest (lowest) wavelength closest to the Controller.
(All sensors are labeled with their individual wavelength included in the part number.)
- 2.** The loss in all interconnecting fiber does not exceed 0.5dB per kilometer, verified by measurement.
- 3.** No fusion splice introduces more than 0.05dB loss. Every splice must be measured for dB loss.

If there is deviation from these preconditions, a full complement of 50 sensors per channel may be possible, but reliable sensing performance with 50 sensors cannot be assured and should not be assumed.

System layouts are configured with sensors connected in either a full daisy-chain or a split daisy-chain; examples of each are shown in Figure 2 and Figure 3. The selected configuration is based on the physical layout of the locations being monitored, and it will be predefined before installation begins. The predefined layout must be closely followed when installing and connecting components.

Figure 2

Full daisy-chain configuration

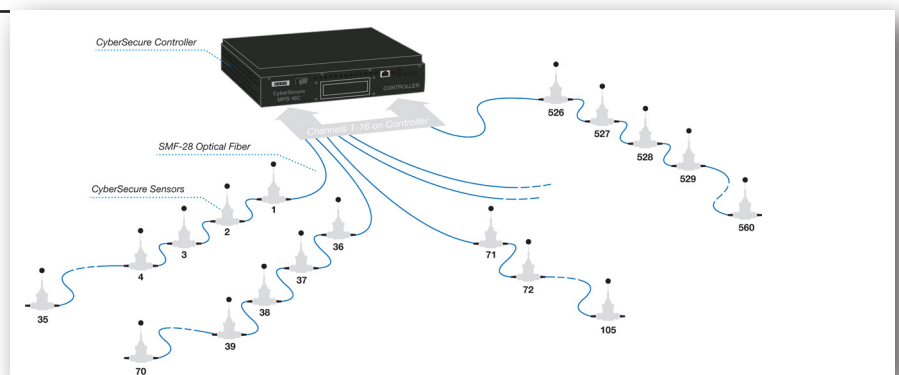
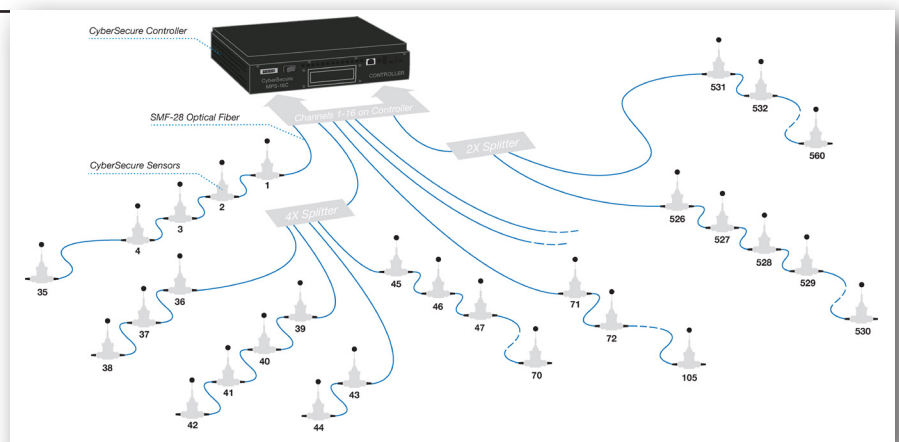


Figure 3

Split daisy-chain, with examples of various valid configurations on individual channels





4. Loss Factors and Maximum Allowable Losses

The performance of an CSMP5-10 system is affected by the losses in the interconnecting fiber and all field splices. Losses must be minimized for optimal system performance; therefore, losses must be known and controlled. Loss factors are discussed below, and maximum allowable losses are summarized in Table 1.

Type SMF-28 fiber is commonly used in telecom systems. If any existing SMF-28 dark fiber already passing through the protected manhole spaces is being used as part of an CSMP5-10 installation, then all such fiber must first be tested from end to end for loss, before splicing in any sensors. The maximum allowable loss in the fiber is 0.5dB per kilometer. If testing confirms the loss does not exceed this value, then such fiber may be utilized as the link between sensors, splitters (if any) and the Controller. Appendix B describes equipment and methods for testing fiber.

If new SMF-28 fiber is installed for an CSMP5-10 system, then the fiber also must be tested from end to end for loss to verify no damage occurred during pulling, before splicing in any sensors. The maximum allowable loss is 0.5dB per kilometer. Appendix B describes equipment and methods for testing fiber.

Splices are the greatest contributor of losses, so quality fusion splices are critically important. Splice losses must be measured, not assumed. The maximum allowable loss per fusion splice is 0.05dB. Because each sensor has two pigtails, this means two splices and a maximum allowable one-way loss of 0.1dB per sensor. Loss in any additional splicing also must be known and accounted for. Extra fiber length should be left at each location in case re-splicing is necessary. See Appendix B for information on measurements.

Medium	Maximum Allowable Loss	Notes
Repurposed dark fiber, SMF-28	0.5dB per kilometer	Measured beforehand
Newly-pulled fiber, SMF-28	0.5dB per kilometer	Measured after pulling into place
Fusion Splice	0.5dB per splice	Measured
	0.1dB per CSMP5-10 sensor	One-way loss through two pigtails

Table 1

Summary of maximum allowable losses

Note:

The pigtails of each CSMP5-10 sensor contain fiber that is polyimide coated. Stripping techniques used for typical acrylate-coated telecommunications fiber do not work (or work very poorly) for polyimide coatings. See Appendix A for information on how to effectively strip the polyimide coating.

All sensors on one Controller channel are 'tuned' to different wavelengths to allow all sensors on that channel to be separately identified and addressed. The sensor wavelengths fall at regular intervals between 1460 and 1620 nanometers. All CSMP5-10 sensors are labeled, and their part number includes their individual wavelength. Table 2 lists all available part numbers. During installation, installers must ensure the wavelength of each sensor matches the intended location in the predefined layout. If a sensor is damaged and must be replaced, then a replacement CSMP5-10 with the same part number (matching wavelength) must be used in that location.

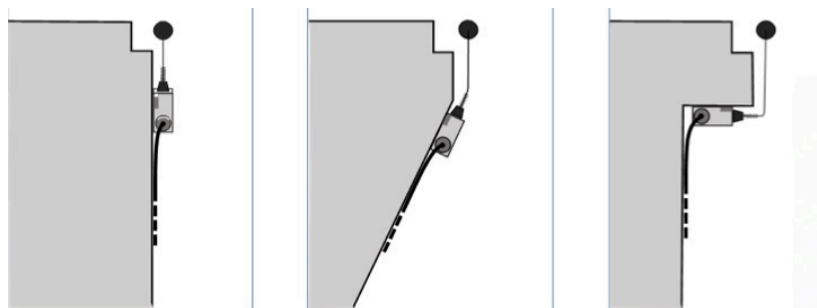
Cyber Sensor Installation Guide

5. Sensor Installation

The A CSMP5-10 sensor is mounted just below the ring in which the manhole cover rests. The side wall profile of a manhole shaft typically is either vertical, or tapered toward a larger diameter shaft with increasing depth, or immediately undercut to a larger diameter shaft; these profiles are illustrated in Figure 5. In general, the sensor body must be mounted approximately 6 inches below the manhole ring seat so that closure of the manhole cover reliably causes the sensor actuator ball and stem to be pushed sideways. The actuator stem on each CSMP5-10 sensor is provided without the ball attached to facilitate bending the stem if necessary to fit the configuration of the manhole. With the sensor body properly mounted, the actuator stem properly bent and the ball installed on the end of the stem, the top of the ball should be roughly even with the top edge of the manhole metal ring, as shown in Figure 4. When installed in a manhole having vertical side walls, the sensor body should be tilted toward one side about 15° to ensure the actuator deflects sideways when the manhole cover is put in place. Sensors may be mounted directly to concrete side walls using anchor bolts screwed into the concrete, such as shown in Figure 5. Sensors also may be mounted using hardware that protects the sensor body and the pigtail exit points, and which is adjustable to fit various manhole configurations; an example is shown in Figure 6. The specific method(s) and hardware will be predefined on the installation configuration drawings.

Figure 4

Manhole profiles and CSMP5-10 sensor placements



After mounting the sensor and bending the actuator stem if necessary, install the ball on the end of the stem by pressing the ball in place until it locks. The spring in the actuator stem accommodates variations in placement and large movements. The ball on the end of the actuator stem is used to increase safety and help ensure deflection despite any recesses that may be cast into the bottom of a manhole cover.

Bring the pigtails down into the manhole, and secure and splice them into SMF-28 fibers using the configuration and components predefined in the system layout documentation (separate from this document).

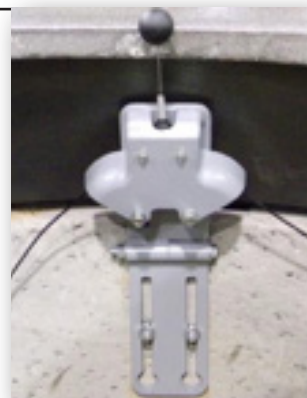
Figure 5

Vertical wall



Figure 6

Protective mounting hardware and adjustable bracket





6. Cyber Sensor Controller

The Cyber Sensor Controller, shown in Figure 8, is basically a “black box” approximately the size of a video disc player. The Controller has an operating temperature range of -20° to +60°C, requires 120VAC power, and must be protected in an enclosure. SMF-28 fiber to/from each group of CSMP5-10 sensors (up to 16 groups, each comprised of up to 50 sensors as previously discussed) ultimately must terminate at the optical Controller which continuously scans them. There are up to 16 numbered LC/APC fiber optic connectors on the back panel of the Controller housing, one connector for each channel. The ‘home run’ optical fiber leading to the first sensor (or a splitter if used) on a given channel connects to the Controller via an LC/APC fiber optic connector. Apart from these connectors at the Controller, all other connections in all optical fibers are via fusion splices as previously stated. Installers must ensure the ‘home run’ fiber from any group of sensors is connected to the proper channel number as defined in the system layout documentation. The Controller communicates with a remote monitoring computer via standard Ethernet. The user interface software resides on the remote monitoring computer, which typically is located in a security monitoring facility. Details on placement of the Cyber Sensor Controller are given in the system layout documentation (separate from this document).

Figure 8

Cyber Sensor Controller



Note:

If conventional telecom OTDR or optical power measuring equipment is used to assess the integrity of the fiber and/or splices, or is used to measure the optical power from the Cyber Sensor Controller present at sensors, some such equipment may give erroneous results. See Appendix B of this document for information on appropriate testing equipment.

CSMP5-10.1461	CSMP5-10.1493	CSMP5-10.1525	CSMP5-10.1557	CSMP5-10.1589
CSMP5-10.1464	CSMP5-10.1496	CSMP5-10.1528	CSMP5-10.1560	CSMP5-10.1592
CSMP5-10.1468	CSMP5-10.1500	CSMP5-10.1532	CSMP5-10.1564	CSMP5-10.1596
CSMP5-10.1471	CSMP5-10.1503	CSMP5-10.1535	CSMP5-10.1567	CSMP5-10.1599
CSMP5-10.1474	CSMP5-10.1506	CSMP5-10.1538	CSMP5-10.1570	CSMP5-10.1602
CSMP5-10.1477	CSMP5-10.1509	CSMP5-10.1541	CSMP5-10.1573	CSMP5-10.1605
CSMP5-10.1480	CSMP5-10.1512	CSMP5-10.1544	CSMP5-10.1576	CSMP5-10.1608
CSMP5-10.1484	CSMP5-10.1516	CSMP5-10.1548	CSMP5-10.1580	CSMP5-10.1612
CSMP5-10.1487	CSMP5-10.1519	CSMP5-10.1551	CSMP5-10.1583	CSMP5-10.1615
CSMP5-10.1490	CSMP5-10.1522	CSMP5-10.1554	CSMP5-10.1586	CSMP5-10.1618

Table 2

Available CSMP5-10 part numbers

The part number format is CSMP5-10.XXXX, where XXXX is the center wavelength of a switch expressed as hundreds, tens, and units of nanometers; the ‘i’ in the thousands place is omitted.

End of general installation instructions. Also see Appendices A and B.

Cyber Sensor Installation Guide

Appendix A

Stripping of polyimide coating from optical fiber

The In the process of manufacturing optical fiber, the glass is coated with a polymer immediately after being drawn as a fiber from the furnace. The polymer coating strengthens and protects the fiber from chemical interactions and mechanical damage, and various polymer coatings are used. Virtually all telecom fiber is coated with an acrylate polymer, and installation personnel may be most familiar with stripping and splicing of fiber having acrylate coating. However, of all polymer coatings commonly used for optical fiber, polyimide offers superior chemical resistance, abrasion resistance and toughness, so polyimide-coated optical fiber is a good choice for industrial sensor applications. The fiber inside all CSMP5-10 sensors is coated with polyimide, and the polyimide coating continues out the pigtails. Polyimide bonds firmly to the glass surface and does not strip from the fiber nearly as easily as acrylate, so different stripping techniques must be used. The following discussion provides comments and suggested techniques that may be used in field situations.

Some techniques will leave the glass fiber unaffected, while other techniques may cause embrittlement of the glass and make the product fragile and prone to breakage when handled. Choose the technique appropriate for the environment and circumstances in which the fiber stripping and splicing occurs.

Mechanical Stripping

Wire strippers do not work. Because of the bond between the polyimide and the glass surface, wire strippers will not completely remove the polyimide layer (no matter how closely the stripper is adjusted), leaving behind “clumps” that still are bonded to the glass. In the process of attempting to strip the polyimide in this manner, the glass is damaged and breakage is almost certain.

Machining, manual: Manually removing the polyimide using a mechanical scraping technique with a razor blade, X-Acto® knife or cutting tool can work, but a microscope, good lighting and a very steady hand are required. Even so, damage to the glass by the cutting tool is likely, making it prone to breakage. This technique may be challenging in field applications.

Machining, automated: Field-portable equipment, approximately the same size as a portable fusion splicer, is available that clamps the fiber and mechanically removes the polyimide coating in a series of precisely controlled rotational shaving steps. The process is automated, so special skills are not required, and the glass is left undamaged and retains its full strength. An example of such equipment is the PCS-100 offered by Fujikura.

Chemical Stripping

Note:

If Proper safety practices should be followed when working with strong chemical reagents. Some jurisdictions may restrict the use or require documentation of chemical stripping processes.

Sulfuric acid: Concentrated hot sulfuric acid ($T=150-180^{\circ}\text{C}$) removes polyimide rapidly. Dip the fiber for a few minutes or until all polyimide is dissolved, then rinse well in deionized water. Then rinse in acetone, then in methanol, and allow to dry. Multiple applications may be required.

Strong bases: Caustic solutions, such as sodium hydroxide, will attack and remove polyimide. However, they also may etch the silica surface and render it prone to breakage, and they generally are not recommended as a removal method.



Appendix A, continued

Thermal Stripping

Gas torch, oxygen/hydrogen: An oxy-hydrogen flame works well in removing polyimide and leaves the final product strong. Caution should be exercised given the inherent hazards in using this type of torch. Care also should be taken to avoid overheating and distortion of the fiber.

Gas torch, propane or butane: Propane-air or butane-air torches are convenient and often work well in removing polyimide, although they may not be as effective as an oxy-hydrogen torch. If the flame is not hot enough, residual polyimide may remain. After exposure to the torch flame, examine the fiber against a white surface and use alcohol wipes to remove any sooty residue that remains on the fiber.

Open flame: Matches and lighters are quick and easy, and generally effective at removing polyimide from fiber, but they may leave the glass surface brittle. They are not recommended if strength of the final product is important. Sooty residue may remain on the fiber; alcohol wipes should be used to remove it.

Electric coil heater: Current run through a coiled nichrome wire, or a nichrome wire wrapped around a quartz insulating tube, makes a resistive coil heater (e.g., a miniature tube furnace) capable of rapidly burning off the polyimide. One must be careful not to touch the glass fiber to the coiled wire or insulating tube, as this will damage the glass surface and make the glass brittle. Residue is common and post-process cleaning with alcohol wipes is generally required.

Electric arc: A plasma arc is effective at burning off the polyimide while leaving the glass strong. If done manually, the plasma removal process can be challenging to control and overheating is difficult to avoid. However, field-portable plasma arc equipment is available that clamps the fiber and surrounds it with a traveling “ring of fire” that removes the polyimide in a precisely controlled manner. The process is automated, so special skills are not required, and the glass is left undamaged and retains its full strength. An example of such equipment is the Fiber Preparation Unit (FPU) II offered by 3SAE.

Splicing Equipment

Performance of an CSMPS-10 system critically depends on quality splices in all fibers used in the system. If legacy two-axis telecom fiber splicing equipment is used when fusion splicing to the fiber pigtails of CSMPS-10 sensors, and/or if the fiber splicer clamps are not of the proper size, unacceptably high losses often result. A three-axis splicer with clamps that properly hold a coated fiber of 190-200micron diameter must be used. For field work the splicer also should have a battery that supports performance in very cold temperatures. Suitable three-axis fiber splicers with appropriately-sized clamps are currently available on the market; examples of reputable equipment manufacturers include Fujikura and Fitel.

Note:

Equipment manufacturers and/or model numbers mentioned in the above discussions are provided as examples for information only. Mention of these product names does not constitute an endorsement of them by CyberSecure IPS. Multiple other products from other manufacturers are available which also are effective in removing polyimide coatings and/or splicing optical fiber, and the reader is encouraged to research and choose from the solutions available.

Cyber Sensor Installation Guide

Appendix B

Equipment for testing integrity of optical fiber and splices, and measuring power

Because the single-mode optical fiber used to interconnect manhole cover position sensors often is the same fiber used for telecom purposes, in many situations personnel already familiar with telecom fiber installation techniques may be called upon to install the manhole cover sensing system fibers. During the splicing of optical fiber, it is common practice in the telecom industry to measure fiber losses and/or verify the integrity of splices by using an optical time domain reflectometer (OTDR), and to measure the optical power present in the fiber using a power meter. An OTDR and power meter can be very useful in verifying the integrity and/or operation of the optical fiber and all splices associated with the sensors in an CSMPS-10 system installation, and installation personnel may already have an OTDR or power meter that they wish to use. However, some OTDRs may not be suitable for testing the integrity of the fiber and splices associated with multiple installed CSMPS-10 sensors, and some power meters may not respond properly to the optical power generated by the CSMPS-10 system Controller.

OTDRs transmit pulses of light out into an optical fiber, and analyze the strength and timing of back - reflections of that light to identify faults and measure losses in the fiber. Each of the fiber Bragg gratings (FBGs) used in CSMPS-10 manhole cover position sensors reflects a very narrow bandwidth of light back toward the source; the reflectance factor commonly exceeds 70% for each individual FBG in its narrow band. The FBGs in CSMPS-10 sensors are individually tuned to reflect at uniquely different wavelengths, but all are generally located within a broad band spanning roughly 1460 to 1620 nanometers (referred to as the '1550nm band'). Therefore, a multitude of sharp reflections (e.g., "spikes") at different wavelengths between 1460 and 1620 nm, and at different distances corresponding on the locations of the individual sensor FBGs on the fiber, will be seen by an OTDR if it operates in the 1550nm band. The OTDR may 'see' only a few FBG reflections if it emits light pulses in a narrow bandwidth, or it may 'see' a multitude of FBG reflections if it emits pulses across a broad bandwidth. Such reflections thus may cause some OTDRs to give confusing or misleading results that suggest faults in the optical fiber and/or poor splices, when in fact the fiber and splices may be fault-free. To avoid potential confusion caused by FBG reflections, it is important to use an OTDR that operates outside the 1550nm band used by the FBGs in CSMPS-10 sensors. Installation personnel should confirm, in advance of testing fiber installations and splicing, the band(s) in which their OTDR operates. Some OTDRs are available that contain two light sources, one operating in the 1310nm band and the other in the 1550nm band, and allow selection of one or the other. Such OTDRs are suitable for testing the integrity of CSMPS-10 sensor fiber runs, provided only the 1310nm source is used. If an OTDR with only a 1550nm band source is used, then the information it provides may be misleading, and a different OTDR that operates in the 1310nm band should be used instead.

The light source in the CSMPS-10 system Controller emits in the 1550nm band, so if an optical power meter is connected to the fiber during sensor installations and used to measure the optical power present, the power meter must respond to the 1550nm band. Some legacy optical power meters used for telecom purposes may have detectors that respond only to wavelengths in the 1310nm band, or to even shorter wavelengths, but such equipment will give falsely low readings when measuring optical power from an CSMPS-10 Controller source. Also, rather than emitting at a constant single wavelength, the light source in the CSMPS-10 Controller repeatedly sweeps in wavelength across the 1550nm band, which may confuse or cause varying readings in some optical power meters. Installation personnel should understand the response characteristics of their power meter before using it to measure optical power produced by an CSMPS-10.

Contact Us

For more information, please visit our website at WWW.CYBERSECUREIPS.COM

or email us at SALES@CYBERSECUREIPS.COM

or call our Sales Team at 1-844-653-1018 | International calls at 1-240-696-1311

CyberSecure IPS | 551 Commerce Drive, Suite B | Upper Marlboro, MD 20774



CYBERSECURE IPS

INFRASTRUCTURE PROTECTION SYSTEM

EXHIBIT 9



CyberSecure CSS CYBER SENSOR SOLUTION

DETECT  PROTECT  SECURE

Meeting the Demand for Highly Scalable, Cost Effective Manhole Intrusion Detection Systems to Protect Against Unauthorized Access, Copper Theft and Vandalism in Real-Time.



Protection of Critical Infrastructure Pathways

The United States has the most robust network of underground critical infrastructure pathways in the world. The underground critical infrastructure pathways are highly utilized by both Government and Commercial customers to provide secure, high-speed communications to nearly every household, business, school, agency and military base in the U.S. Although the underground critical infrastructure pathway system is critical for our country to function on a daily basis, it is one of the least protected, highly vulnerable infrastructure assets in the country. Due to the rising value of copper over the last 10-years there have been a sky-rocketing number of pathway intrusions through manhole access points that have crippled commercial communications throughout major cities and jeopardized classified communication links for government agencies. These intrusions cost Government and Commercial customers hundreds of millions of dollars every year.

CyberSecure CSS™ (Cyber Sensor Solution) from CyberSecure IPS™ addresses the underground critical infrastructure pathway vulnerabilities by providing 24/7/365 intrusion detection monitoring of manholes, handholes and communication junction sites using powerless fiber optic sensors. The CyberSecure CSS™ hardware controller monitors thousands of CyberSecure CSS sensors and is managed by CyberSecure IMS™ (Infrastructure Monitoring System). CyberSecure IMS™ automates intrusion alarm dispatching, controls case management, provides detailed maps of every manhole and handhole and seamlessly integrates into existing dispatching systems. CyberSecure CSS™ can cost effectively protect critical infrastructure pathways. Protecting manholes, handholes and communication junction sites with CyberSecure CSS™ can save Government and Commercial customers millions of dollars annually by preventing copper theft, vandalism, tampering and unauthorized access.

The United States has the most robust underground critical infrastructure pathway system in the world.

CyberSecure CSS™ addresses the critical infrastructure vulnerabilities by providing 24/7/365 Intrusion Detection Monitoring.

CyberSecure CSS™ Solution Overview

The suite of CyberSecure CSS™ fiber optic sensors is based on state of the art fiber optic technology and use light to sense position. CyberSecure CSS™ sensors contain no electronic components, require no electrical power, and emit no signals. Because no electricity is involved at any CyberSecure CSS™ sensor location, the sensors are intrinsically safe under all conditions. A CyberSecure CSS™ system will continuously monitor the position of manhole and handhole covers and immediately report a change at any cover. Thousands of covers may be monitored simultaneously, and every cover is individually identified and mapped. Individual identification allows exact location of any attempt to access underground communication systems through a manhole and/or handhole on which a sensor has been installed, and facilitates an immediate focused response by security or law enforcement personnel via the CyberSecure IMS™ Alarm Management software application.

CyberSecure CSS™ Sensors

CyberSecure CSS™ sensors utilize a single strand of standard single-mode fiber (SMF) and are immune to electromagnetic and radio frequency interference, emit no signals, and cannot be bypassed without detection. CyberSecure CSS™ sensors are environmentally rugged, with an IP66 industrial standard package configuration, and may be integrated into virtually any manhole and/or handhole. CyberSecure CSS™ sensors are designed for the varying environmental conditions often found in manholes and handholes. They have an operating temperature range of -40° to +80°C (-40° to +176°F) and an operating life of one million cycles. A representative CyberSecure CSS™ sensor is shown in Figure 1.



Figure 1. Universal CSS™ sensor

CyberSecure CSS™ Controller

The CyberSecure CSS™ Controller, shown in Figure 2, connects the sensors using SMF-28 fiber to/from each group of CyberSecure CSS™ sensors (up to 16 channels, each comprised of up to 50 sensors). The CyberSecure™ controllers come in 8-Channel (400+ sensors) and 16-Channel (800+ sensors) models. The CyberSecure CSS™ controller has an operating temperature range of -20° to +60°C (-4° to +140°F), requires 120VAC power, and can be installed indoors or outdoors (must be protected in an enclosure). The controller communicates with CyberSecure IMS™ via standard Ethernet.



Figure 2. CyberSecure CSS™ Controller

CyberSecure IMS™ Alarm / Dispatch Management Application

CyberSecure IMS™ is a U.S. Government certified alarm / dispatch management software application designed specifically to manage the protection of classified communication networks. The Department of Defense, Special Operations Command, Defense Information Systems Agency (DISA) and major government System Integrators all over the world use CyberSecure IMS™ to protect their critical infrastructures. CyberSecure IMS™ offers comprehensive monitoring of all manholes and handholes with integrated geospatial mapping technology, pinpoint location detection of alarmed manholes, real-time alarm notification via phone, text, email and seamlessly integrates into customizable site specific alarm response and inspection procedures.



Figure 3. CyberSecure IMS™



CyberSecure IMS™ can integrate into almost any existing dispatching systems and offers remote users distributed monitoring capabilities over web browsers, phones, and tablets.

CyberSecure CSS™ Installation Configuration Options

All CyberSecure CSS™ sensors are delivered with two pre-installed armored fiber optic pigtailed with essentially no loss, onward to other sensors as required. The pigtailed are available in whatever length is necessary and specified at the time of order.

The pigtailed must be spliced into SMF-28 single-mode optical fiber which in turn either terminates at the CyberSecure CSS™ Controller or leads to other CyberSecure CSS™ sensors. Up to 35 sensors may be connected to one channel of the CyberSecure CSS™ Controller. These connections may be done in either a full daisy-chain configuration or a split daisy-chain configuration. The choice of configuration depends on what works best for the physical topology of the manhole and handhole locations being monitored.

In a **full daisy-chain configuration**, one pigtail on the first sensor connects to one CyberSecure CSS™ Controller channel via SMF-28 optical fiber, and the other pigtail on the first sensor connects (via SMF-28 fiber) to the second sensor on that channel; the second sensor connects to the third sensor on that channel, and so on up to a maximum quantity of 35 sensors on that channel. This is repeated for each of the other CyberSecure CSS™ Controller channels as required. The full daisy-chain configuration is shown diagrammatically in Figure 4, with a CyberSecure CSS™ Controller polling a full complement of 560 manhole cover position sensors; all of the sensors on each channel are connected in daisy-chain.

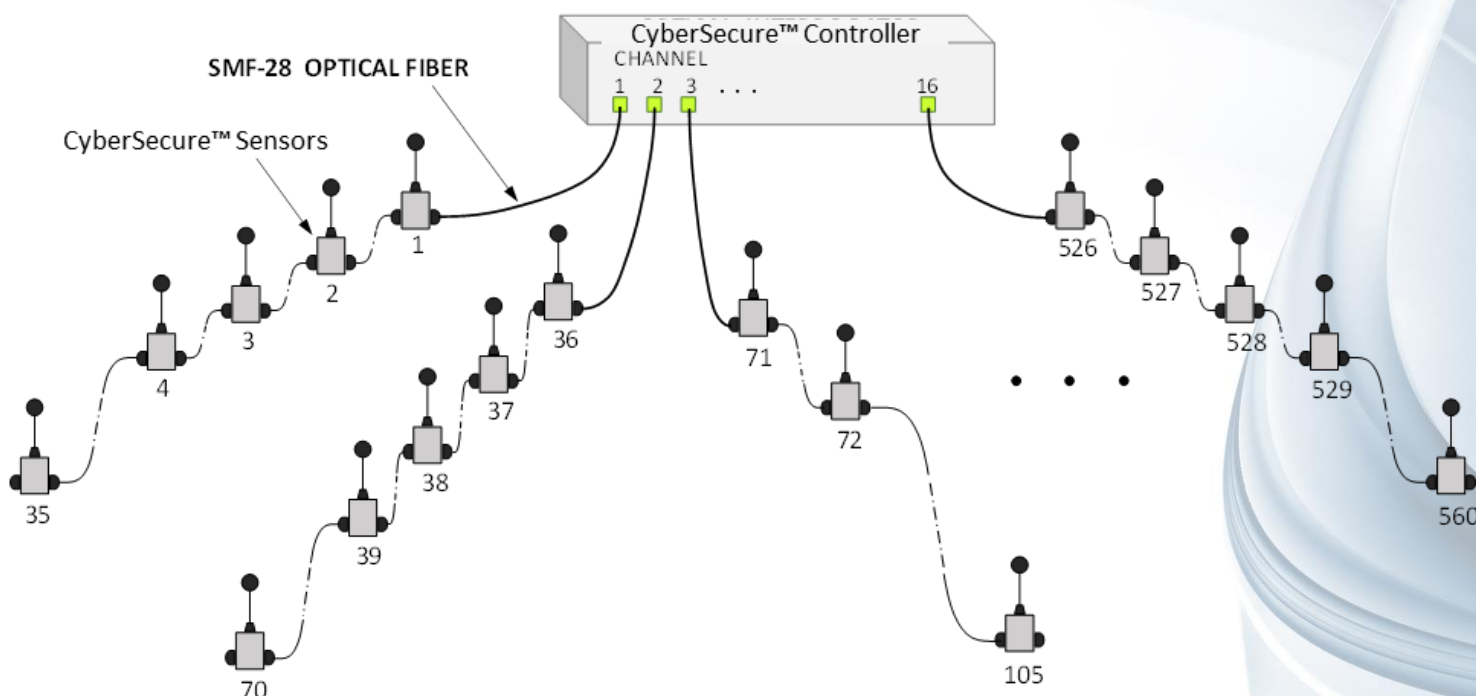


Figure 4. Full daisy-chain configuration



In a **split daisy-chain configuration**, the SMF-28 fiber from one CyberSecure CSS™ Controller channel is connected to a splitter having multiple branches, and each branch in turn is connected to a group of sensors that is connected in daisy-chain. If desired, some CyberSecure CSS™ Controller channels can be configured as a split daisy-chain while other channels are configured as a full daisy-chain. For those CyberSecure CSS™ Controller channels on which a splitter is used, the number of daisy-chained sensors in groups on splitter branches need not be equal. As with a full daisy-chain configuration, the total quantity of sensors per interrogator channel in a split daisy-chain configuration does not exceed 35. A split daisy-chain system with various valid channel configuration examples is illustrated in Figure 5.

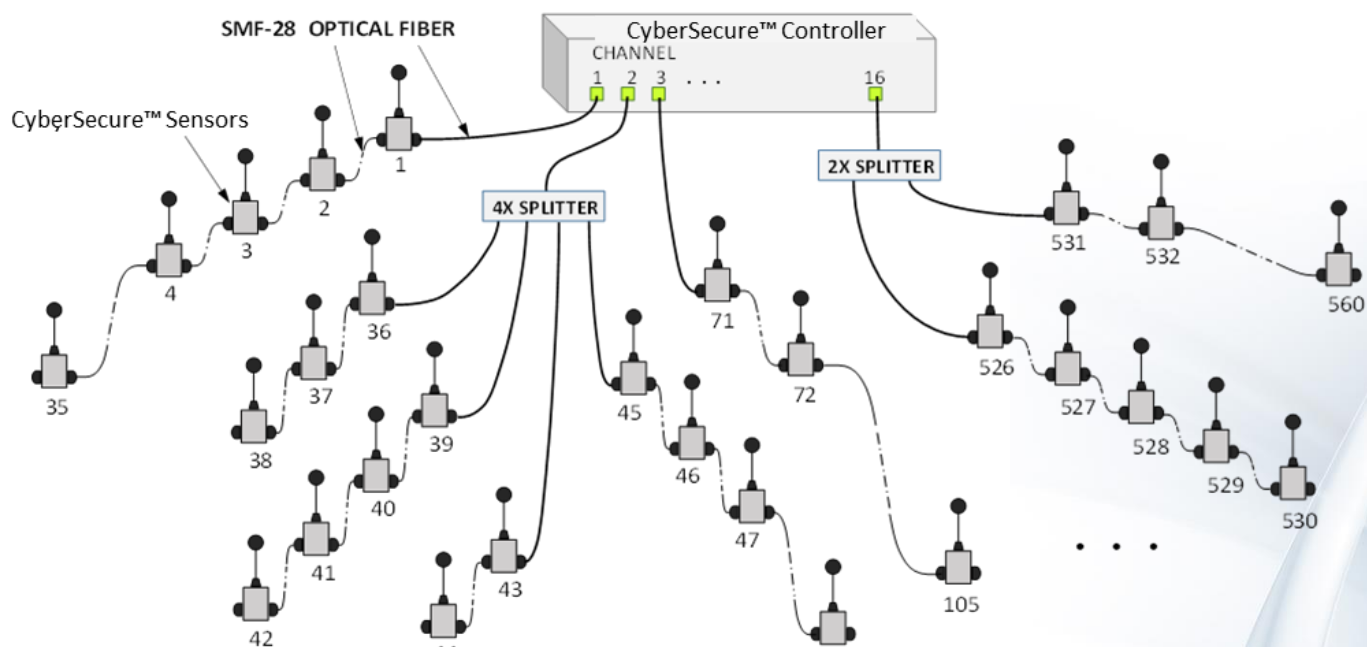


Figure 5. Split daisy-chain configuration

CyberSecure CSS™ Sensor Installation

CyberSecure CSS™ sensors are mounted just below the perimeter seat on which manhole and handhole covers rest. From the perimeter seat location downward, the profile of the side wall of a manhole shaft typically is either vertical, or tapered toward a larger diameter shaft with increasing depth, or immediately undercut to a larger diameter shaft. These profiles are illustrated in Figure 6.

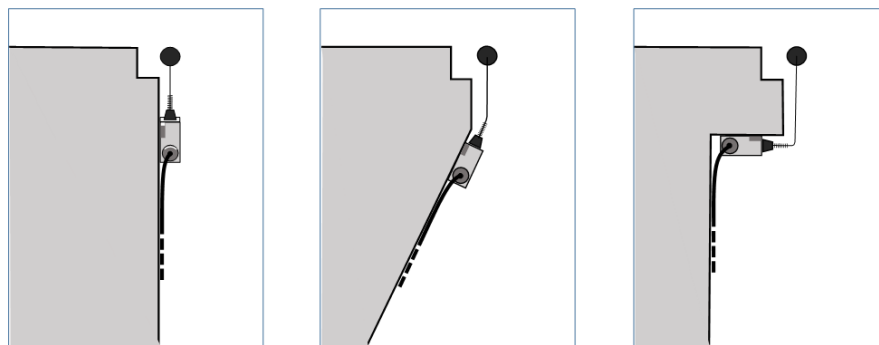


Figure 6. Manhole side wall profiles and CyberSecure CSS™ sensor placements



The CyberSecure CSS™ sensor body has two mounting ears near the top of the package, one on either side. To mount a sensor, choose a suitable location in the manhole shaft where concrete anchor bolts may be used to secure the sensor body; for vertical and tapered side walls the location generally should be no more than 6 inches below the perimeter seat for the manhole cover. The location must be chosen so that, when the sensor actuator stem is bent and/or cut and the ball is installed on the end of the stem, the center of the ball will be approximately even with the top edge of the manhole metal rim.

An example installation of a CyberSecure CSS™ sensor on a vertical wall is shown in Figure 7.



Figure 7. Vertical wall installation

CyberSecure IPS™ Lifecycle Services

CyberSecure IPS™ realizes the importance of post deployment support when protecting the United States' critical infrastructure assets. We offer OEM certified support and training services to ensure each project is successful for the long term.



Figure 8. Lifecycle Services



CyberSecure IPS™ Global Network Operations Center

CyberSecure IPS offers a secure Technical Assistance Center (TAC) and can replicate issues quickly. Our Secure video teleconferencing system enables collaborative support and training to include recorded training sessions that can be viewed at a later date. CyberSecure IPS' Customer Proof of Concept (CPOC) lab allows our engineering staff to deploy your configuration and any updates at our facility prior to deploying it at your site.



Figure 9. Global Network Operations Center

Thank You for the Opportunity to Share Our Solutions!

For more information please visit our website at
www.cybersecureips.com, email us at sales
@cybersecureips.com or contact our sales team at
1.844.653.1018!



CYBERSECURE IPS
INFRASTRUCTURE PROTECTION SYSTEM