

Express Mail ED 232665020 US

Before the  
Federal Communications Commission  
Washington, D.C. 20554

RECEIVED & INSPECTED  
OCT 14 2005  
FCC - MAILROOM

In the Matter of the Appeal of the	)	File No. SLD -
	)	
Decision of the	)	
	)	
Universal Service Administrator by	)	
	)	
<b>Dublin City School District</b>	)	
	)	
Federal-State Joint Board on	)	
	)	CC Docket No. 96 - 45
Universal Service	)	
	)	
Changes to the Board of Directors of	)	
	)	
The National Exchange Carrier	)	CC Docket No. 97 - 21
	)	
Association, Inc.	)	

**Appeal**  
and  
**Demand for Expedited Relief**

October 11, 2005

Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
445 12th Street, S.W. Suite TW-A325  
Washington, D.C. 20554

This is an appeal and request for expedited relief from a decision by the  
Schools and Libraries Division of the USAC to the Federal Communications  
Commission.

No. of Copies rec'd 0+4  
List A B C D E

Enclosed are the original and four copies of the Appeal. An extra copy is also enclosed; please time stamp the extra copy and return it to me in the enclosed self addressed-stamped envelope.

**(1) Funding Commitment Decision Letter Appealed**

Form 471 Application Number:	82116
Funding Year 2005:	07/01/2005-06/30/2006
Billed Entity Number:	127425
Date of Funding Denial Notice:	September 8, 2005
Date of Appeal:	October 11, 2005

**(2) SLD Contact Information**

Demme M. McMannus  
Technology Director  
Dublin City School District  
(478) 277.9802 x215  
207 Shamrock Dr.  
Dublin, GA 31021-3020

**(3) Funding Request Numbers Appealed**

FRN – 1334480

**(4) The SLD stated that funding is denied because:**

“30% or more of this FRN includes a request for application software, which is an ineligible product based on program rules.”

**(5) The SLD was provided very precise data to support Applicants’ request for funding FRN – 1334480.**

**Exhibit A** is an Item 21 Attachment to the FCC Form 471.

The SLD did not ask one question of either the Enterasys & FortiGate (manufacturers), Progressive Communications, Inc. (vendor) or Dublin on this issue.

### **Argument**

First, "Firewall" is defined by the FCC as:

#### **"Description:**

A firewall is a hardware and software combination that sits at the boundary between an organization's network and the outside world, and protects the network against unauthorized access or intrusions.

#### **Eligibility:**

A firewall is eligible for discount if it provides basic and reasonable security protections to prevent unauthorized access to the information, software, and systems of an applicant's eligible components."

*Schools and Libraries' Eligible Services List for Funding Year 2006 – Page 34, Internal Connections.*

Second, Item 21, Exhibit A, sets forth all the detail that the SLD required for an analysis to determine fundability. However, since apparently no analysis is available for this appeal, I will set forth Dublin's item by item support.

- a. Dragon Enterprise Management Server Appliance. The manufacturer's website demonstrates that this is hardware. **Exhibit B**
- b. Dragon GE250 Network Sensor Appliance (Fiber NIC). This is hardware that allows a fiber connection to the network, not software. **Exhibit C**
- c. NetSight Atlas Automated Security Manager. This is precisely what determines when the network is being attacked. It is the purpose of the firewall. **Exhibit D**

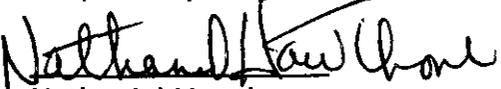
- d. FortiManager (Management Platform for UT 25 nodes) This item is software; when used in conjunction with the FortiGate 400 provides protection from attacks. **Exhibit E** It is fundable; how even if not fundable, at \$14, 495, 00, it's certainly not 30% of the cost (Total Cost: \$396,740.00).

**Conclusion:**

Dublin is requesting the following action by the FCC:

- (a) Find that the detail that Dublin provided supports the Application.
- (b) Within 30 days or less Order funding for telecommunications services requested in the 471 Application, specifically FRN – 1334480
- (c) Set aside funds to totally fund the Dublin request.

Respectfully submitted,

  
Nathaniel Hawthorne

Ohio Bar # 0008881  
Nathaniel Hawthorne,  
Attorney/Consultant, Ltd.  
27600 Chagrin Blvd., #265  
Cleveland, OH 44122  
tel.: 216/514.4798  
nhawthorne@earthlink.net

Attorney for  
Dublin City School District  
Cc: Dublin City School  
District

**Exhibit A**



**Exhibit B**

## Specifications

### Technical Specifications

---

#### Dragon EFP Appliance

Architecture: Intel Pentium 4  
Memory: 2 GB, minimum 73.4 GB hard drive  
NICs: 2 10/100/1000Base-T copper

#### Dragon Enterprise Management Server Appliance

Architecture: Dual Intel XEON  
Memory: 2 GB, minimum 73.4 GB hard drive  
NICs: 2 10/100/1000Base-T copper

#### Dragon Enterprise Management Server Redundant Appliance

Architecture: Dual Intel XEON  
Memory: 2 GB, minimum (2) 73.4 GB hard drives, RAID 1  
NICs: 2 10/100/1000Base-T copper

#### Integrated Network Sensor/Server

Architecture: Intel Pentium 4  
Memory: 2GB, minimum 36 GB hard drive  
NICs: 2 10/100/1000Base-T copper, and 1  
10/100/1000Base-T copper or 1 1000Base-SX fiber

### Environmental Specifications

---

#### Operating Temperature

+5° C to +35° C (41° F to 95° F)  
(maximum change not to exceed +10° C)

#### Non-Operating Temperature

-40° C to +70° C (-40° F to 158° F) (ambient)

#### Non-Operating Humidity

95% at 35° C (non-condensing)

#### Power Consumption

Voltage Range: 4.96 Amp at 115V  
Voltage Range: 2.48 Amp at 220V

### Agency and Standards Specifications

---

#### Safety

Argentina: IRAM Certificate  
Canada: UL60950-CSA 60950 (UL AND cUL)  
China: GB4943 (CCC certification)  
Europe/CE Mark: EN60950 (complies with 73/23/EEC)  
Germany: GS License  
International: IEC60950 (CB Report and Certificate)  
Nordic Countries: EMKO – TSE (74-SEC) 207/94  
Russia: GOST 50377-92  
U.S.: UL60950 – CSA 60950 (UL and cUL)

#### Electromagnetic Compatibility (EMC) (Class A)

Australia/New Zealand: AS/NZS 3548 (based on CISPR 22)  
Canada: ICES-003  
China: GB9254 and GB17625 (CCC CERTIFICATION)  
Europe/CE Mark: EN55022, EN55024 and  
EN61000-3-2;-3-3 (complies with 89/336/EEC)  
International: CISPR 22  
Japan: VCCI  
Korea: RRL, MIC 1997-41 and 1997-42  
Russia: GOST 29216-91 and 50628-95  
Taiwan: CNS13438  
U.S.: FCC, Part 15

## Exhibit C

## Specifications

### Technical Specifications

---

#### IDS Software

##### Dragon Network Sensor Software for Ethernet

Part Numbers: DSNS7-E

Performance rating: 20 Mbps

##### Dragon Network Sensor Software for Fast Ethernet

Part Numbers: DSNS7-FE

Performance rating: 200 Mbps

##### Dragon Network Sensor Software for Gigabit Ethernet

Part Numbers: DSNS7-GE

Performance rating: 1 Gbps or greater

Network Sensor Software is supported on the following operating systems:

Fedora Core, Redhat Enterprise, Sun Solaris

### Technical Specifications

---

#### IDS/IPS Appliances

##### FE100 Dragon Network Sensor Appliance

Part Numbers: DSNSA7-FE100-TX

Performance rating: 100 Mbps

Architecture: Intel Celeron

Memory: 1 GB, 40 GB IDE hard drive

NICs: 2 10/100 copper, 1 10/100/1000 copper

Plus, 1 10/100/1000 copper for IPS appliance

(2 ports on the IPS are fail-safe bypass)

##### GE250 Dragon Network Sensor Appliance

Part Numbers: DSNSA7-GE250-TX/SX

Performance rating: 250 Mbps

Architecture: Intel Pentium 4

Memory: 1 GB, minimum 36 GB hard drive

NICs: 2 10/100/1000 copper, plus 1 Gigabit fiber or 1

Gigabit copper NIC configuration

Plus, 1 10/100/1000 copper for IPS appliance

(2 ports on the IPS are fail-safe bypass)

##### GE500 Dragon Network Sensor Appliance

Part Numbers: DSNSA7-GE500-TX/SX

Performance rating: 500 Mbps

Architecture: Dual Intel XEON

Memory: 1 GB, minimum 36 GB hard drive

NICs: 2 10/100/1000 copper, plus 2 Gigabit fiber or 2

Gigabit copper NIC configuration

(2 ports on the IPS are fail-safe bypass)

##### GIG Dragon Network Sensor Appliance

Part Numbers: DSNSA7-GIG-TX/SX

Performance rating: 1+ Gbps

Architecture: Dual Intel XEON

Memory: 2 GB, minimum 36 GB hard drive

NICs: 2 10/100/1000 copper, plus 4 Gigabit fiber or 4

Gigabit copper NIC configuration

Redundant power and cooling standard

(4 ports on the IPS are fail-safe bypass)

### Physical Specifications

---

#### Form Factor

1U rack-mount server chassis for EIA standard 310-D racks

#### Dimensions

4.32 cm (1.7") H X 42.9 cm (16.9") W X 58.42 cm (23")

D (FE100 only)

4.32 cm (1.7") H X 42.9 cm (16.9") W X 60.71cm (23.9") D

2U rack-mount server chassis for EIA standard 310-D racks

#### Dimensions

8.8 cm (3.4") H X 42.9 cm (16.9") W X 60.71cm (23.9") D

#### Front Panel (Buttons)

Power on/off button, system-reset button, ACPI sleep switch system ID button, and tool-activated NMI switch (FE100 only)

#### Front Panel (LEDs)

Power, hard drive activity, network activity (two), and general system fault

### Environmental Specifications

---

#### Operating Temperature

+5° C to +35° C (41° F to 95° F)

(maximum change not to exceed +10° C)

#### Non-Operating Temperature

-40° C to +70° C (-40° F to 158° F) (ambient)

#### Non-Operating Humidity

95% at 35° C (non-condensing)

#### Power Consumption

Voltage Range: 4.96 Amp at 115V

Voltage Range: 2.48 Amp at 220V

## Exhibit D



[Home](#)

[Products/Services](#)

[Training](#)

[Support](#)

[Partners](#)

[Company Info](#)



You are Here: [Products](#) > [Management](#) > [Enterasys NetSight® Automated Security Manager](#)

**New Products!**

[NetSight Console 2.0](#)  
[NetSight Automated Security Manager](#)

**Enterasys Management**

[NetSight Console](#)  
[NetSight Automated Security Manager](#)  
[NetSight Router Services Manager](#)  
[NetSight Inventory Manager](#)  
[NetSight Policy Manager](#)  
[Service Options](#)

**Service Resources**

[NetSight Policy Manager and User Personalized Network Assessment, Design and Implementation Services](#)  
[Service Contract Product Registration](#)

**Management Resources**

[Awards-Test Results](#)  
[Customer Testimonials](#)  
[Downloads](#)  
[Certification and Training](#)

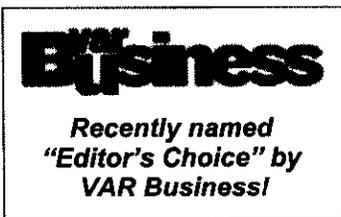


**Product Datasheet PDF**

[Features & Benefits](#)  
[Technical Specifications](#)  
[Ordering Info](#)  
[Screen Shots](#)  
[Free Evaluation!](#)  
[Show All](#) | [Hide All](#)

# Enterasys NetSight® Automated Security Manager

NetSight Automated Security Manager is the industry's first security application to make the critical connection between infrastructure and security. To do this, NetSight Automated Security Manager uses a revolutionary new technique to integrate the switching and routing infrastructure with Dragon™ Intrusion Defense technology, providing the ability to take action on the port on which an attack is identified.



NetSight Automated Security Manager takes security events from Dragon Intrusion Defense, locates the exact port on the Matrix™ switch where attacks are entering the network, and takes action on the port, stopping the threat. Using a "quarantine role" for the user connected to the port, the Matrix switch can dynamically deny, limit or change the characteristics of the user's access to the network.

NetSight Automated Security Manager is the industry's first product to stop threats and protect network and business operations dynamically.

NetSight Automated Security Manager is part of the NetSight enterprise-class network management system that provides command and control of a Secure Networks infrastructure.

It is the first in a series of new Enterasys security applications designed to support Secure Networks.

**Exhibit E**



**FortiGate Solutions**

- SOHO Office
- Enterprise
- Service Provider

**Our Products: Fortinet > FortiManager**

**Fortinet FortiManager System**

The FortiManager System is an integrated management and monitoring tool that enables enterprises and service providers to easily manage large numbers of FortiGate Antivirus Firewalls. It minimizes the administrative effort required to deploy, configure, monitor, and maintain the full range of network protection services provide by FortiGate devices, supporting the needs of enterprises and service providers responsible for establishing and maintaining security policies across multiple, dispersed FortiGate installations.

**FortiGate Firewalls**

- FortiGate 50A
- FortiGate 60
- FortiWiFi 60
- FortiGate 100
- FortiGate 200
- FortiGate 300
- FortiGate 400
- FortiGate 500
- FortiGate 800
- FortiGate 1000
- FortiGate 3000
- FortiGate 3600
- FortiGate 4000



**Fortinet FortiManager, 25 FortiGate Managed Nodes**

FortiManager System is an integrated management and monitoring tool that enables enterprises and service providers to easily manage large numbers of FortiGate Antivirus Firewalls. It minimizes the administrative effort required to deploy, configure, monitor, and maintain the full range of network protection services provide by FortiGate devices, supporting the needs of enterprises and service providers responsible for establishing and maintaining security policies across multiple, dispersed FortiGate installations.

**Add-ons & Upgrades**

- FortiManager
- FortiLog
- FortiReporter
- FortiClient
- FortiGuard

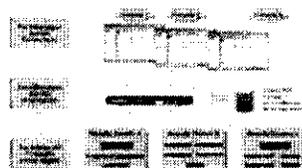


**Fortinet FortiManager, 100 FortiGate Managed Nodes**

FortiManager System is an integrated management and monitoring tool that enables enterprises and service providers to easily manage large numbers of FortiGate Antivirus Firewalls. It minimizes the administrative effort required to deploy, configure, monitor, and maintain the full range of network protection services provide by FortiGate devices, supporting the needs of enterprises and service providers responsible for establishing and maintaining security policies across multiple, dispersed FortiGate installations.

**FortiCare Support**

- 8X5 Support
- 24X7 Support



**Fortinet FortiManager, 200 FortiGate Managed Nodes**

FortiManager System is an integrated management and monitoring tool that enables enterprises and service providers to easily manage large numbers of FortiGate Antivirus Firewalls. It minimizes the administrative effort required to deploy, configure, monitor, and maintain the full range of network protection services provide by FortiGate devices, supporting the needs of enterprises and service providers responsible for establishing and maintaining security policies across multiple, dispersed FortiGate installations.

**Fortinet FortiManager, 500 FortiGate Managed Nodes**

FortiManager System is an integrated management and monitoring tool that enables enterprises and service providers to easily manage large numbers of FortiGate Antivirus Firewalls. It minimizes the administrative effort required to deploy, configure, monitor, and maintain the full

**Fortiwall.com**  
Internet Security Experts

Have a Question? Call 800-558-3302

Search for:



HOME SOLUTIONS PRODUCTS SUPPORT LEARNING CENTER COMPANY PARTNERS

CHECKOUT MY ACCOUNT

FortiGate Solutions [Our Products: Fortinet > FortiGate Firewall](#)

SOHO Office  
Enterprise  
Service Provider

### FortiGate 400 Firewall

Product SKU: FG-400-US

#### FortiGate Firewalls

- FortiGate 50A
- FortiGate 60
- FortiWiFi 60
- FortiGate 100
- FortiGate 200
- FortiGate 300
- FortiGate 400
- FortiGate 500
- FortiGate 800
- FortiGate 1000
- FortiGate 3000
- FortiGate 3600
- FortiGate 4000



#### DOCUMENTATION

- [FortiGate 400 Datasheet](#)
- [FortiGate Interface Demo](#)
- [Multizone Tech Note](#)

#### Configuration Service

Have your new firewall configured by our Fortinet trained experts. [Learn More](#)

>>

**For guaranteed lowest pricing please Request a Quote or Call Toll-Free 800-558-3302**



#### Add-ons & Upgrades

- FortiManager
- FortiLog
- FortiReporter
- FortiClient
- FortiGuard

#### FortiCare Support

- 8X5 Support
- 24X7 Support

FortiGate™ Antivirus Firewalls are dedicated, hardware-based units that deliver complete, real-time network protection services at the network edge. Based on Fortinet's revolutionary FortiASIC™ Content Processor chip, the FortiGate platforms are the only systems that can detect and eliminate viruses, worms, and other content-based threats without reducing network performance – even for real-time applications like Web browsing. FortiGate systems also include integrated firewall, content filtering, VPN, intrusion detection and prevention, and traffic shaping functions, making them the most cost effective, convenient, and powerful network protection solutions available.

The FortiGate 400 Antivirus Firewall meets enterprise-class requirements for security, performance, flexibility, and reliability. Flexible deployment options allow FortiGate users to customize ports and assign Route and NAT mode options to individual interfaces. The FortiGate 400 Antivirus Firewall provides granular security through multi-zone capabilities, which allows administrators to segment their network into zones and create policies between zones. Featuring 4 auto-sensing 10/100 Base-T Ethernet ports, the FortiGate 400 offers award-winning network-based antivirus, firewall, content filtering, VPN, network-based intrusion detection and prevention, and traffic shaping services. Additionally, the FortiGate 400 supports high availability operation with stateful failover to a redundant stand-by unit. The FortiGate 400 is kept up to date automatically by Fortinet's FortiProtect Network, which provides continuous updates that ensure protection against the latest viruses, worms, Trojans, and other threats – around the clock, and around the world.

#### Product Highlights:

- Provides complete network protection functionality through a combination of network-based antivirus, web content filtering, firewall, VPN, and network-based intrusion detection and prevention, and traffic shaping
- Eliminate viruses and worms from email, file transfer, and realtime (Web) traffic without degrading network performance
- Front-panel LCD and keypad ease deployment by setting basic system parameters without an external console