SR16692007   ##1421H221A##

ACN Communications
170 Chastain Meadows Ct
Kennesaw, GA 30144

CTN3100376   SR16692007   Rev 0

Service Request

ACN Helpdesk #: 866-561-0005

SR Type: Unspecified Time and Material (T&M)   Dispatch Type: (null)

Reference Number: 9813005   End User Reference:

Date: 05/24/2021   Window: 13:00 to 13:00 EDT   Expected Duration: 234   PO#:

Site Contact: CATHERINE   Phone: 5162805142   Alt. Phone:

Company: ACN Repair   Address: 233 WESTBURY BLVD

City: Hempstead   State: NY   Zip: 11550

TAC: 404.536.4721 (AT&T) | 678.332.8358 (Verizon) | 678.460.2530 (Other)

SR DETAILS

DESCRIPTION OF WORK

MAKE SURE TO CALL END USER WHILE EN ROUTE TO SITE.

SR CHECKLIST

1. Call Genesis +1.800.493.0016 to log onsite
2. Refer to the attached install guide for specific installation instructions.
3. Verify all installation areas are clean and that you properly dispose of all trash.
4. Please submit all deliverables
5. Leave site.
6. Submit all Post Visit Completion (PVC) tasks within 24 hours of logging off site.

To be completed by the Field Engineer (FE): 43398

Call Result:	[ ] Successful [ ] Incomplete	Incomplete Reason:	Installed Equipment:

Materials Used:

Description	Qty

Required for all calls:

Time at Log-on: _____:_____ EDT

Time at Log-off: _____:_____ EDT

Customer Heldesk Rep. Name: _____

Customer Call Closure Code: _____

Onepath TAC Rep. Name: _____

Onepath TAC Closure Code: _____

Installed Equipment:

Make/Model	Serial Number

RMA Equipment:

Make/Model	Serial Number

FE Initials	End-User Name (Please Print)	Title	End-User Signature	Date

Description: Complete SOW as described on your SR. Dispatch can consist of wiring, device installation, or troubleshooting.
Required Tools: Standard Telco + Dispatch Specific Requirements
Required Materials: Standard Telco + Dispatch Specific Requirements
Required Skills: Telecom & Networking
RMA Handling: DO NOT REMOVE ANY EQUIPMENT FROM SITE. Neatly pack equipment, then provide to POC
FE Overage Threshold: 2 hours

Customer has passed the Covid-19 Security Questions.

Equipment:

March 11, 2021

Re: COVID 19 - City/County/State/Federal Orders

To whom it may concern:

Please be informed that the bearer of this letter is subcontracted by Genesis Networks, a communications and information technology company providing essential critical infrastructure as outlined by the Cybersecurity and Infrastructure Security Agency (CISA); an agency operating under the Department of Homeland Security.

Under CISA guidelines, these workers must be able to travel to and gain access to infrastructure facilities and offices during curfews and restricted travel periods. CISA identifies the following list as essential to continued critical infrastructure:

Communications:

• Maintenance of communications infrastructure- including privately owned and maintained communication systems- supported by technicians, operators, call-centers, wireline and wireless providers, cable service providers, satellite operations, undersea cable landing stations, Internet Exchange Points, and manufacturers and distributors of communications equipment

• Workers who support radio, television, and media service, including, but not limited to front line news reporters, studio, and technicians for newsgathering and reporting

• Workers at Independent System Operators and Regional Transmission Organizations, and Network Operations staff, engineers and/or technicians to manage the network or operate facilities

• Engineers, technicians and associated personnel responsible for infrastructure construction and restoration, including contractors for construction and engineering of fiber optic cables

• Installation, maintenance and repair technicians that establish, support or repair service as needed

• Central office personnel to maintain and operate central office, data centers, and other network office facilities

• Customer service and support staff, including managed and professional services as well as remote providers of support to transitioning employees to set up and maintain home offices, who interface with customers to manage or support service environments and security issues, including payroll, billing, fraud, and troubleshooting

• Dispatchers involved with service repair and restoration

Information Technology:

• Workers who support command centers, including, but not limited to Network Operations Command Center, Broadcast Operations Control Center and Security Operations Command Center

• Data center operators, including system administrators, HVAC & electrical engineers, security personnel, IT managers, data transfer solutions engineers, software and hardware engineers, and database administrators

• Client service centers, field engineers, and other technicians supporting critical infrastructure, as well as manufacturers and supply chain vendors that provide hardware and software, and information technology equipment (to include microelectronics and semiconductors) for critical infrastructure

• Workers responding to cyber incidents involving critical infrastructure, including medical facilities, SLTT governments and federal facilities, energy and utilities, and banks and financial institutions, and other critical infrastructure categories and personnel

• Workers supporting the provision of essential global, national and local infrastructure for computing services (incl. cloud computing services), business infrastructure, web-based services, and critical manufacturing

• Workers supporting communications systems and information technology used by law enforcement, public safety, medical, energy and other critical industries

• Support required for continuity of services, including janitorial/cleaning personnel

All persons performing critical operations have been instructed to comply with hygiene and social distancing requirements as established by the Centers for Disease Control and Prevention.

Please do not hesitate to contact me should you have any questions regarding this letter or our operations.

Sincerely,

Bryan Hann

Area Vice President – Deployed Services, Genesis Networks

May 27, 2020

To Whom It May Concern:

The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issues this letter to facilitate work in the interest of homeland security by Communications Sector workers identified in the CISA Essential Critical Infrastructure Workers advisory guidance, dated May 19, 2020.[1] CISA requests any courtesy that can be extended to essential workers involved in communications infrastructure operations, maintenance and restoration **in response to the COVID-19 Pandemic and any other regional disasters (e.g., hurricanes, tornadoes, wildfires, earthquakes) that may occur during any COVID-19 response phase**.

CISA developed the **Essential Critical Infrastructure Workers** advisory guidance identifying workers that conduct a range of operations and services deemed essential to continued critical infrastructure viability. This list is intended to support State, local, tribal, and territorial officials' decision-making as they work to protect their communities, while ensuring continuity of functions critical to public health and safety, as well as economic and national security.

In developing this advisory guidance, CISA determined that essential workers need access to jobsites based on our judgment that organizations affiliated with the Communications Sector engage in activity that could reasonably be included within the scope of "critical infrastructure" as that term is defined in law; and critical communications infrastructure is necessary to ensure first responder, emergency responder, and 911 communications capabilities are functional during this response and recovery period. In the course of providing this support, identified Essential Critical Infrastructure Workers in the Communications Sector should be able to travel to and access necessary critical infrastructure facilities in order to prevent loss of service or restore critical communications services.

CISA greatly appreciates your cooperation. For any questions or concerns related to this request, please contact the CISA at 888-282-0870 or CISAservicedesk@cisa.dhs.gov.

Sincerely,

Christopher C. Krebs
Director
Cybersecurity and Infrastructure Security Agency (CISA)

---

[1] "Guidance on the Essential Critical Infrastructure Workforce," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/publication/guidance-essential-critical-infrastructure-workforce.

Closure Details

Representative	Group	Closure Code / Hold Time
Ex: Bob Smith	*NOC*	*BS1215 / 10 min*

Milestone	Time
Ex: Time Onsite	*10:00*
Ex: Time Offsite	*12:15*
Time Onsite	
Time Offsite	

Time Breakdown (Send using myESP)	Reason
Example: 10:00-11:00	*Arrival onsite, extending demarc from back of store to front counter*

Equipment Installed (Make/Model)	Serial Number
Example: Cisco 1941	*FTX1254789*

Materials Used	QTY	Material Provider
Example: Cat5e UTP	*127 ft*	*FE* / *Onepath* / *Customer*
Cat5e UTP		FE / Onepath / Customer
RJ-45 jacks		FE / Onepath / Customer
RJ-11 jacks		FE / Onepath / Customer
Other:		FE / Onepath / Customer
Other:		FE / Onepath / Customer

Equipment Disposition Form

Instructions: Please fill out this form upon completion of the installation for unused/defective gear that may need to be returned based upon the specific RMA handling instructions for this customer. You will be responsible for completing the following:

1. Determine if there are any unused or defective items that may need to be returned.
2. Record the make, model and serial number of each return device in the EQUIPMENT INFORMATION section below.
3. Record the equipment type in the EQUIPMENT INFORMATION section below. "Defective" refers to an out-of-box failure for customer supplied equipment. "Unused" refers to gear that was shipped to site by the customer but was not used to successfully convert the site (this should be *extremely* rare).
4. Securely pack the CPE in the box the new equipment came in and upload a photo of the equipment in the box before sealing to myESP.
5. **Review your SR details and look for the RMA handling section. This will provide instructions on how to handle the equipment return. You may need to ship the equipment back to Onepath or leave it with the site contact. MAKE SURE TO CHECK YOUR SR FOR INSTRUCTIONS!**
6. Fill out the CONFIRMATION section and ask the MOD to sign the equipment return form to indicate acceptance and understanding of the process. Advise the site contact how the defective/unused equipment should be handled (left onsite for safe keeping, you are taking offsite for return or the device should be handed to FedEx for a call tag return).

EQUIPMENT INFORMATION

Make/Model	Serial/ID No.	Equipment Type
		**Defective	Unused**
		**Defective	Unused**
		**Defective	Unused**
		**Defective	Unused**
		**Defective	Unused**
		**Defective	Unused**
		**Defective	Unused**
		**Defective	Unused**
		**Defective	Unused**

CONFIRMATION

SR Number				
Date			**Site Contact Name**	
RMA handling process	Leave with MOD	FE drop off required	Call tag		
Installer Name			**Site Contact Signature**	
Installer Signature				