NSSLGlobal

ON LAND ▮ ONBOARD ▮ ONLINE

SMART@SEA

powered by NSSLGlobal

Seamless management of communications and IT services

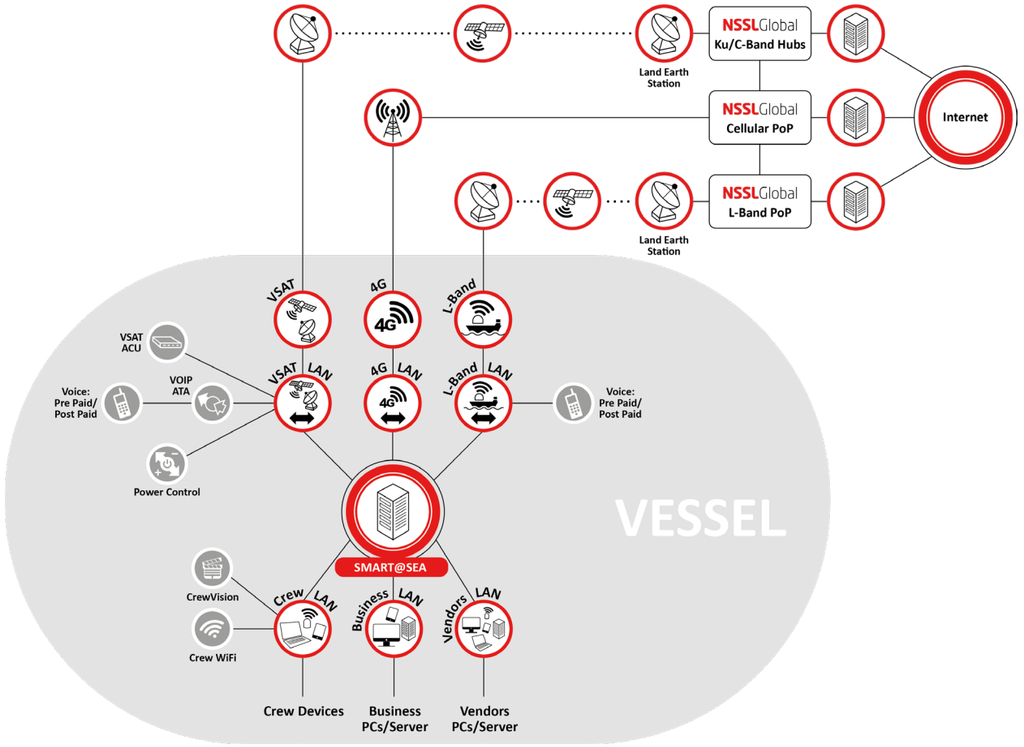
A virtualised environment

SMART@SEA is NSSLGlobal's next generation intelligent evolution of the industry-proven Cruise Control+. It is a powerful cost-effective, single server solution for the seamless integration of communications, cybersecurity, IT services and crew welfare services.

It enables remote deployment and delivery of new value-added services and managed services with no additional hardware, all delivered through the single virtual appliance.

NSSLGlobal's SMART@SEA appliance is installed locally on-board the vessel and is designed to help maritime customers manage their vessels' business, vendor and crew welfare networks thus ensuring maximum efficiency and cost-effectiveness.

Providing both flexibility and security, the SMART@SEA appliance provides customers with a product to assist them on their road to becoming IMO Cyber compliant as well as providing access to a suite of additional Value-Added Services and Managed Services.



SMART@SEA
powered by NSSLGlobal

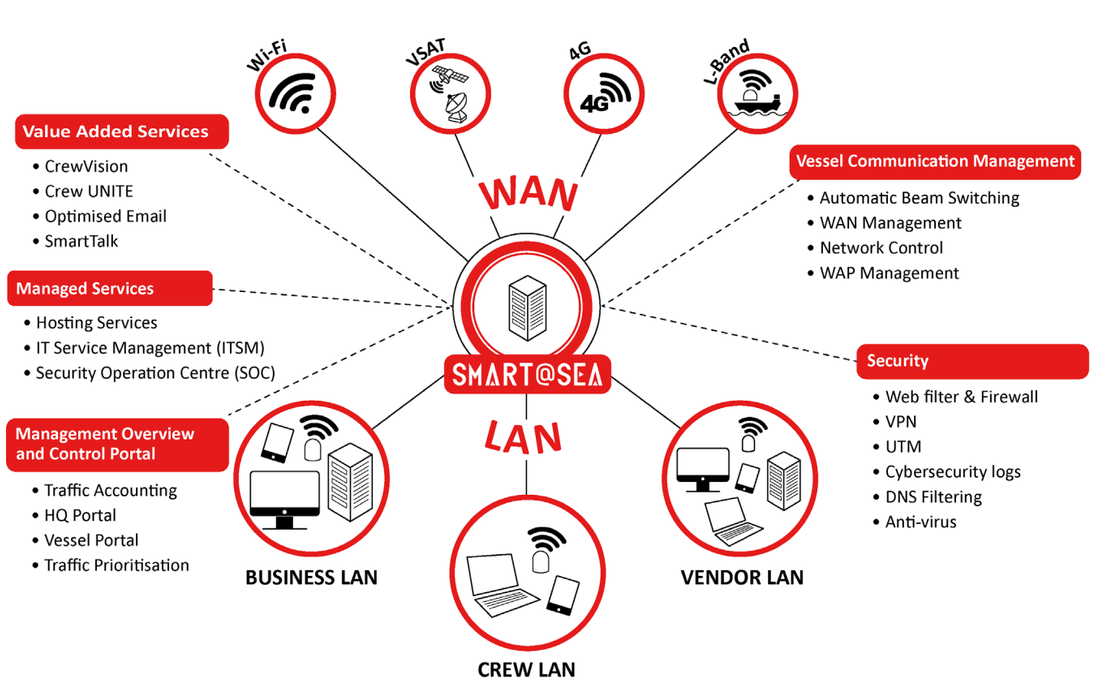
Complete end-to-end solution

SMART@SEA is designed to give maritime customers complete control regardless of the satellite or terrestrial communications system on-board.

Within a single appliance, the virtualised platform offers a complete solution, from vessel communications management, vessel level security, a management control portal, computer hosting, IT Service Management and a Security Operations Centre service.

SMART@SEA provides maritime customers with the flexibility to deploy customer specific applications on-board, without additional hardware thereby offering greater support capabilities, space savings and improved capacity management. In addition, the managed hosting aids the customer by managing the virtual hardware and operating system on- board, freeing up their time to focus on vessel priorities.

The SMART@SEA solution automatically applies security patching and software upgrades which take effect 'over the air' via our unique SatLink multicast solution outside of the customers data package, providing no disruption to their service.



SMART@SEA
powered by NSSLGlobal

Vessel communications management

The core SMART@SEA service provides seamless management of the communication bearer.

AUTOMATIC BEAM SWITCHING (ABS)

ABS provides continuity of service to the customer while traversing between VSAT coverage areas. This is all managed without any interaction from the crew on-board who can spend time focusing on critical duties.

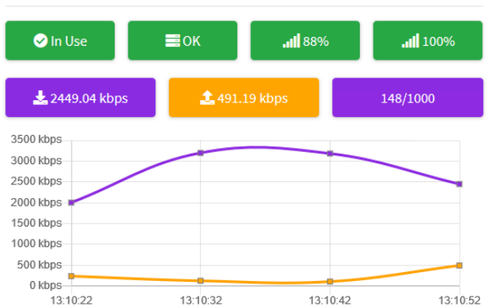
WAN MANAGEMENT

When the vessel's primary communication bearer (VSAT, 4G, L-Band or shoreside WiFi) is offline or in blockage, corporate network traffic is routed using NSSLGlobal's SMART@SEA to the on-board communications backup carrier. Unlimited secondary connections such as L-Band, LTE services and Wi-Fi are available for the customer to select which ensures the highest availability to the vessel if primary services are unavailable.

This also allows NSSLGlobal to utilise the backup system for remote diagnostics and fault rectification thereby again reducing the need for crew interaction.

NETWORK CONTROL

NSSLGlobal provides as many completely segregated on-board networks as required (ie for Business, Crew and Vendor). Each on-board network is kept secure from the other on-board networks. IP addresses are assigned automatically or manually. The Captain has complete overview of the network which allows them to enable/disable segments and devices as required.



VSAT WAN status

WAP CONTROL - SECURITY

Wireless access points are managed, monitored and disabled centrally via the Vessel Portal. NSSLGlobal can provide intelligent WAPs which locally filter Layer 7 protocols and integrate with the UTM to provide intelligent protection.

A compliant, secure on-board solution

NSSLGlobal has been serving some of the world's largest governments with secure solutions for over 50 years. Our security and communications solutions assist with compliance for the IMO 2021 guidelines by providing both equipment and services to both detect and counter threats to your network integrity.

In addition to the security our products provide, they are all installed and administered by security cleared staff and engineers, many of whom have first-hand experience of being mariners and working in the field.

The following critical security controls are the core components of NSSLGlobal's solutions, ensuring customers are able to maintain full control of your network and infrastructure:

1. NETWORK SEPARATION AND SEGMENTATION ensures that all core function, critical data and operations local area networks are separated from crew welfare traffic and non authorised access. Each LAN can be also be customised with specific rules for QoS to optimise bandwidth against bearer availability.

2. MALWARE PROTECTION AND PREVENTION scans all incoming traffic to application level, detecting and removing suspected malware, with inbuilt Ransomware, Botnet and Phishing protection. In addition, DNS requests are filtered to prevent access to and downloads from suspicious URLs.

3. EDUCATION AND TRAINING helps raise awareness of the potential cyber risks, allowing crew and vessel owners to both be more prepared to mitigate against them and to understand their role in keeping the system secure.

4. INTRUSION DETECTION monitors all traffic and server devices by ensuring the applications and services are displaying normal behaviour patterns as well as all requests going to and from the network to ensure any malicious software, applications or traffic is spotted and either acted on or notifications are issued.

5. REGULAR SOFTWARE UPDATES mean the system is always prepared, even against the latest emerging threat. All NSSLGlobal Solutions receive regular software updates across our IT Infrastructure and customer networks to ensure the latest security patches are always in place. In additional, our customer anti-virus offerings for both gateway and clients are dynamically kept up to date every 2 hours to ensure its awareness of possible threats is as comprehensive as possible.

6. SIEM AND LOG MANAGEMENT ensures security logs are monitored to allow notifications and centralised monitoring and reporting of incidents and events on the clients, servers and devices on the network, ensuring compliance with regulatory requirements.

CYBER SECURE NSSLGlobal

CYBER ESSENTIALS PLUS

CERTIFIED ISO 27001:2021 COMPANY

Vessel security controls

SERVICES	BENEFITS
Network device IP assignment	The SMART@SEA network device IP function provides complete control of IP assignment for the vessel's networks: ▪ Control of all devices accessing the business, crew or vendor networks ▪ Automatic assignment of the IP address; no action required to manually configure each device connecting to the network
Firewall	▪ SMART@SEA gives control of the IP addresses and ports which can access the system, essentially which devices or routes are allowed to communicate both in and out of the SMART@SEA ▪ Segregates and secures all on-board networks (business, crew and vendor), restricting and allowing traffic to specific IP addresses and network ports/services ▪ NSSLGlobal's firewalls operate over any carrier, including the primary (VSAT IP@SEA), backup (Inmarsat/Iridium/LTE), and other bearers, allowing us to provide a stable, reliable and secure platform on the vessel
Anti-Virus: Including scanning of email attachments	Powerful, rapid anti-virus scanning. The security software will scan all incoming traffic to the vessel as well as connected end point devices, removing malicious files and malware in the quickest time possible at a pre-arranged schedule. Prevents malicious file types from being sent to clients via email
DNS Filter	Prevents IP Spoofing by verifying the DNS address of requested websites against an online verified repository
Web Filter	Provides control of the websites, or categories that clients can browse, including http and https* sites (* proxy required for https traffic)
Web filter scanning of file downloads	Prevents malicious file types from being downloaded to help prevent infection of the client's device
VPN	Allows secure encryption of business traffic between the vessel and the client's HQ or other specified destination
Vessel Portal	Allows the captain or authorised personnel to control elements of the service on-board
Firewall and web filtering scheduling	Provides the ability to schedule firewall and web filtering rules at certain times of the day
Cybersecurity logs	Enables the customer to see all cybersecurity activities, which can be viewed within the vessel portal or sent automatically to HQ for review
Unified Threat Management (UTM)	Provides a local layer 7 UTM firewall that delivers the following: ▪ Enhanced firewall ▪ Gateway anti-virus ▪ Wi-Fi Management ▪ Enhanced QoS ▪ Intrusion detection and prevention capabilities on all assets on the network ▪ Deep packet inspection for application-level analysis, enabling blocking of certain applications across the bearer for example Skype or iTunes and ensuring bandwidth is available for key applications
HQ Portal	Allows the HQ (or NSSLGlobal at the request of HQ) to view and change the configuration of security controls on each vessel or group of vessels
Network Control	NSSLGlobal provides as a standard, six completely segregated on board local area networks (i.e. for Business, Crew and Vendor). Each on-board network is kept secure from other networks and can be disabled by the Captain using the vessel portal. Each network is monitored by the AV/UTM as part of the secure environment
Hosted applications and IT Management service	NSSLGlobal can host and manage your applications, therefore ensuring cybersecurity is managed and the appropriate controls are in place
Intruder detection and Intruder protection	The on-board network environment is constantly monitored. Any new devices, logins or network activity the security software doesn't recognise and authorise will instantly be blocked

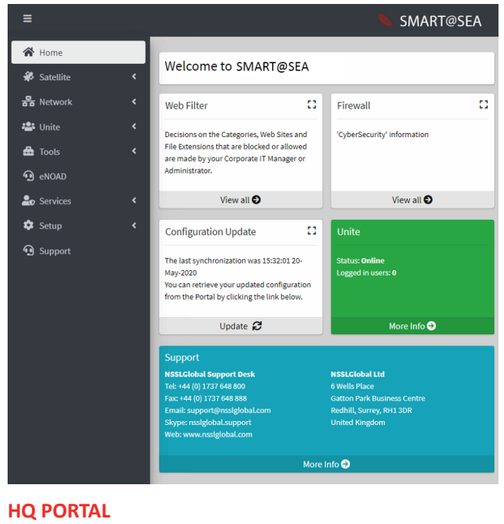
Management control and overview

VESSEL PORTAL

The SMART@SEA appliance provides a local vessel portal that enables the Captain to monitor and maintain control over the on-board networks and satellite link at any time.

In addition to any monitoring function the Captain has, NSSLGlobal constantly monitor the end-to-end service. NSSLGlobal pride themselves on proactive monitoring and can see immediately if a vessel has a service issue so can start working to resolve the issue, very often before the vessel even knows the service is unavailable. Should performance degradation be seen, NSSLGlobal will investigate by remotely accessing the vessel or by arranging a proactive service visit at a suitable port of call.

The suite of tools available means that NSSLGlobal are able to detect and rectify traffic issues/bottlenecks, malicious traffic types (malware, botnets, virus) and Peer2Peer using Layer 7 signature and interrogate the live traffic and historic traffic to/from the vessels. On the hub side NSSLGlobal are able to monitor our SatLink equipment at our hubs and the satellite router on the vessel. NSSLGlobal can monitor both RF and IP usage and performance metrics. These include RX/TX burst errors, RX/TX signal levels, current FEC rate, statistics (RX/TX rate), packet delivery statistics, TCP PEP statistics, live TCP connection statistics, and QoS utilisation.



HQ PORTAL

The SMART@SEA portal gives the shore side HQ a holistic view and real-time visibility into the different data services running on the vessel as a way of managing and controlling the bandwidth usage on- board. The portal allows the HQ (or NSSLGlobal at the request of HQ) to view and change the configuration of controls on each vessel or group of vessels. Users and or departments can be provided with granular access, enabling them to view and modify the permissions on specific vessels within a fleet.

TRAFFIC ACCOUNTING

The traffic accounting function provides the ability to have oversight usage of all on-board networks separately. This can report billing data and graphs at the desired time and frequency and even enable onward billing to a third-party vendor if required.

Value added services and crew welfare

CREWVISION

CrewVision is NSSLGlobal's integrated ship entertainment system offering a wide variety of viewing content which is continually updated to the vessel via a multicast function of the VSAT IP@SEA network without any impact to the user experience on-board. CrewVision provides on-demand access to a wide variety of movies, TV drama box sets, documentaries, sports and daily news. The service is provided either in communal areas on-board or can be viewed by the crew's own personal mobile device.

CREW UNITE

When crew are away at sea they can maintain contact with home using our Crew UNITE service. We provide a Wi-Fi hotspot voucher system enabling crew to purchase internet and voice vouchers for their personal devices. Voucher status can be viewed at any time by the Crew Member whilst in use. Utilising Crew UNITE assists with the responsible use of the VSAT by crew, ensuring bandwidth availability for priority traffic.

EMAIL

Our robust Email service provides compression and resilience over a high latency network. Customers can choose to use their own POP3/SMTP client, they can also utilise a bespoke email domain for vessel addresses, or use the SMART@SEA email domain. Email file size limits can also be set on each WAN connection to ensure bandwidth is managed effectively and that bill shock does not occur when not utilising the primary connection.

SMARTTALK

The new integrated and cost effective SmartTalk PBX provides customers with the opportunity to move from analogue phones to IP phones enabling better mobility for users on the vessel as well as calls within the vessel. This PBX solution reduces the implementation time and costs as the IP connectivity can be via existing network cables or Wi-Fi without the need to run additional analogue cabling. This also provides the ability to allow Corporate Users and Crew Users to use analogue handsets, or their own cell phones smartphones and tablets to make calls thereby removing the need for additional on-board crew kiosks.

Managed Services

In a world where everybody expects their IT systems to work seamlessly, it is crucial that vessels are supported 24/7. It may be that the customer's IT teams are occupied with daily operations and this is where our range of managed services can assist customers with computer hosting, IT service management and Security Operations Centre service.

COMPUTER HOSTING

Our computer hosting function provides customers with options for hosting a customer Windows Server solution as well as a managed anti-virus solution for clients onboard the vessel, all optimised to work efficiently over satellite.

The integration of customer specific applications into the managed platform, enables saving of both space and crew resource on-board. Additionally, the use of software based utilities allows over-the-air updates that would be difficult to achieve for on-board isolated hardware solutions.

IT SERVICE MANAGEMENT (ITSM)

NSSLGlobal can also provide a range of ITSM services that will assist customers with improving their ability to deploy, integrate and manage their IT systems. With a mixture of agents and agentless collection allowing the collection of key Window O/S events to a central portal that can be viewed by the customer.

Example events that could be monitored;

- Windows Services
- CPU, RAM, Hard Disk usage
- Hardware/power failures
- Network utilisation

Key areas of improvement for ITSM can be;

- Operational excellence
- Ensuring end-users have the best experience possible
- Ensuring processes are in place and working efficiently
- Transparency of activities

SECURITY OPERATIONS CENTRE (SOC)

NSSLGlobal offer a SOC managed service that works alongside the customer to monitor and improve its security and visibility while preventing, detecting, analysing, and responding to cybersecurity incidents across all managed connections, fleets & vessels.

The NSSLGlobal SOC incorporates our internal and customer facing information security teams. The team is made up of both our security technicians and security engineers/analysts that oversee the security operations for both our organisation and our customer's infrastructure.

Working closely and in conjunction with the normal NSSLGlobal NOC, support and customer response teams, The SOC can rapidly respond to any security incident in a concise and coordinated way. we find this combined approach, allows cybersecurity incidents to be quickly and effectively addressed.

Types of SOC monitoring performed;

- Site Survey (remote)
- Installation (remote)
- Preventative Maintenance
- Continuous Proactive Monitoring
- Alert ranking and management
- Threat Response
- Recovery and Remediation
- Log Management
- Root Cause Investigation
- Compliance management

Vessel safety management and IMO 2021

The greater shift towards interconnectivity at sea offers many benefits in terms of cost-efficiency and flexibility for maritime operations, but it also opens up a whole host of vulnerabilities, putting vessels under the threat of cyber-attacks. Poor security has resulted in some high-profile attacks leading to significant loss of customer and industry confidence, reputational damage, severe financial losses and penalties, and litigation affecting the companies involved.

IMO CYBER RISK MANAGEMENT RESOLUTION

In June 2017 the IMO adopted Resolution MSC.428 on Maritime Cyber Risk Management in Safety Management Systems. This resulted in the issuance of compliance structure and date for compliance. The resolution states that an approved safety management system should include cyber risk management in accordance with the objectives and requirements of the ISM Code, no later than the first annual verification of a company's Document of Compliance after 1 January 2021.

WHAT DOES THIS MEAN FOR VESSEL OWNERS AND OPERATORS?

The introduction of the IMO guidelines for cybersecurity brings requirement for both attitudes and methodologies towards cybersecurity at sea to change. Moving forward, the objectives and requirements listed within the ISM code are to be the key components when considering risk assessment for on-board systems. These requirements will need to be met for the vessel to approved during annual class authority review. Responsibilities for the vessel operator now include:

- Roles and responsibilities must be clearly designated, both on-board and at HQ
- Ensure that adequate risk assessments are carried out when considering cybersecurity
- Cyber risk management methods are to be included in the vessel Ship Management System
- Cybersecurity must be considered as part of the safety mechanism on-board, it becomes the Master's responsibility to oversee
- All crew must be trained on cybersecurity, ensuring awareness of requirements and measures to take if required
- The vessel systems must be configured and located correctly to ensure safe operation, separating access from non-authorised personnel
- All IT and communications equipment must be certified as compliant, with assurance from the third-party supplier provided

WHAT IS NSSLGLOBAL DOING TO SUPPORT OUR CUSTOMERS?

As an end-to-end provider of communications and IT services to the maritime market NSSLGlobal has to ensure its services are compliant according to the IMS code. This involves regular reviews of our systems and processes to rectify obsolete and unsupported software that forms part of the customer supply chain.

NSSLGLOBAL CYBER COMPLIANT SOLUTIONS

SMART@SEA provides customers with key security controls, ensuring customers are able to maintain full control of their network and infrastructure. With its Computer Hosting, SOC and ITSM services it can also help the customer on their road to cyber compliancy.

SMART@SEA includes the following Cyber services to help customers build a secure solution on-board and assisting with their IMO 2021 Cyber compliance.

SMART@SEA - IMO Protection	
Fully supported Hardware	✓
Supported and updated OS	✓
Software Patching Mechanism	✓
Network Protection – Layer 3 firewall (CC)	✓
URL Web Filter	✓
DNS Filter	✓
Security Information and Event Management (SIEM)	✓
Botnet protection	✓
Ransomware defence	✓
End Point Status monitoring and reporting	✓
Regular Anti-virus updates (up to 2 hourly)	✓
Network Protection – Layer 7/Application Firewall (UTM)	✓
Rapid AV Scanning and reporting	✓
Multiple Network Monitoring	✓
IDS and IPS	✓
VM Support	✓
VPN	✓
VM security integration	✓
Remotely Configurable solution	✓
24/7 Support	✓
Crew training and Best Practice videos	✓

Best Practice: A new way of thinking and operating

The introduction of the IMO resolution for cybersecurity brings requirement for both attitudes and methodologies towards cybersecurity at sea to change. Moving forward, the objectives and requirements listed within the ISM code are to be the key components when considering risk assessment for on-board systems. These requirements will need to be met for the vessel to be approved during annual class authority review.

The cybersecurity solutions and services provided by NSSLGlobal conform to both industry and IMO standards. However, the responsibility for vessel implementation remains with the vessel owner/operator. Our products and systems form part of a larger interconnected eco-system, which must include secure designs of networks and addressing uncontrolled access to the internet, as well as monitoring of how devices on-board are utilised and the way in which crew members react to the threat.

Ultimately, all of the measures described in this brochure must form part of a vessel safety management system which must be implemented on-board, ensuring both the vessel and the owner are protected at all times. As experts both in the integration of maritime equipment and cybersecurity, NSSLGlobal can help.

NSSLGlobal has produced a series of guides and videos on the best practices at sea that can be provided free of charge upon request.

For further details please contact marketing@nsslglobal.com

Why NSSLGlobal?

Technical Support

55 Years + of Industry Experience

State of the art Monitoring Tools

Security Approved Support Teams

Cyber Certified

NSSLGlobal

ON LAND ▮ ONBOARD ▮ ONLINE

UK - Redhill (HQ) Tel: +44 (0) 1737 648 800 • **UK - Newcastle Tel: +44 (0) 191 296 1658**
UK - Cornwall Tel: +44 (0) 1737 648 800 • **UK - Portsmouth Tel: +44 (0) 1737 648 800**
Germany - Hamburg Tel: +49 40 68277-0 • **The Netherlands Tel: +31 (0) 8507 34010**
Denmark Tel: +45 3670 3603 • **Poland Tel: +48 22 404 78 64**
Norway Tel: +47 67 535 337 • **Singapore Tel: +65 6358 3991**
Sweden Tel: +46 31 990 777 **USA Tel: +1 (504) 305 6185**

marketing@nsslglobal.com

www.nsslglobal.com

V3.260824