The services required in each Grid shall, at any time be expected to include, but will not be limited to the following:

* Research/investigations of the metal market and recycling industry in South Africa to determine the destination of stolen Eskom equipment.
* The profiling of criminal syndicates and unscrupulous scrap metal dealers
* Profiling thieves not related to criminal syndicates within communities involved with theft of Eskom Network Infrastructure.
* The use of informers within the communities involved with the theft of Eskom Network Infrastructure.
* Policing of the Provincial Disposal Contract/ensure effective control of Eskom material and equipment through appropriate commercial procedures.
* Investigate criminal activities committed by metal merchants, smelters, exporters, metallurgical laboratories, relating to the trading, transporting or handling of stolen Eskom equipment.
* Investigate Eskom internal misconducts and criminal activities committed by employees and contractors, as and when reported.
* Provide written progress report on the investigation to the responsible Eskom Line Manager/Requestor.
* Compile a comprehensive investigation report with detailed findings and recommendations for action/implementation by Eskom.
* Research/investigations into the activities of criminal elements and crime syndicates targeting
* Eskom network infrastructure by means of obtaining intelligence and putting an end to these crimes and identifying criminals for criminal prosecution.
* Eskom material identification statements in support of criminal investigations and prosecution upon recovery.
* Interact with law enforcement agencies to provide training where identified and to create awareness on the impact of the crime.
* Interaction with the judiciary to provide training and support where required.
* Develop appropriate technology solutions in support of this strategy.
* Identify hotspots where equipment theft syndicates and petty thieves who are not syndicates, are operating and initiate intelligence driven operations to apprehend them.
* Attend and participate at SAPS disruptive operations in various areas.
* Compile and maintain case dockets with sufficient evidence to apprehend and initiate prosecution, or to take other necessary action against the above.
* Submit processed evidence to relevant government authorities for appropriate action.
* Monitor and support relevant government authorities during above-mentioned action.
* Maintain a database to log all information gathered during the above research/investigations.
* Provide Eskom with intelligence which may be used to establish an in house active crime – intelligence capability.
* Establish measures to counter act the prevalence of corruption in relation to crimes of this nature.
* The service provider shall have an existing electronic database of the criminals, suspects, syndicates, groups, assets recovered, arrests, and convictions.
* The service provider will supply a dual server that can be housed in a safe location decided by Eskom to enable Eskom to access the data without delays. Access levels to the electronic database will be decide on and managed by Eskom Grid Security Manager.
* Provide Eskom with access to content – e.g. Read/View rights on incident management system / existing database containing syndicates, suspects, scrap Dealers, Eskom Hot spots and modus operandi’s of suspects
* The service provider shall have an air surveillance capability fitted with night vision – preferably doing so by using drones, mainly for overhead lines and in mountainous areas.
* The service provider is to furnish Eskom with electronic backups of all data gathered on monthly basis.
* The service provider shall have at least 5 years of provable experience of investigating and or dealing with non-ferrous infrastructure vandalism and thefts.
* The service provider should have a legal team at their disposal experienced in criminal law with a particular focus on network infrastructure crime and criminal matters amendment act. The team must have the ability to initiate court proceedings, both civil and criminal and must be able to assist in the recovery of proceeds of crime with the assistance of Asset Forfeiture Unit.
* Monitor and investigate illegal exports of non-ferrous metals at all ports of exits.
* Monitor the syndicate members after their release from prison.
* The service provider must support the criminal justice system during the criminal prosecution process, and act as a custodian in criminal cases on behalf of Eskom. They must be able to give sound advice to National Prosecuting Authority and SAPS concerning the best cause of action in the matters.
* The service provider will arrange for the centralisation of criminal cases from various areas with the assistance of the NPA and SAPS to ensure the most effective way of prosecuting criminals.
* The service provider must conduct syndicate mapping and evidence analysis.
* Identify metallurgical laboratories/scrap metal dealers, smelters in the Western Cape and other provinces if so required, that are involved in the handling and or processing of scrap metal scrap destined for the export market.
* Identify and Profile perpetrators/syndicates of Network Infrastructure Crime
* Identify Crime Hotspots/Risk Areas where infrastructure crime syndicates are operating
* Identify the Modus Operandi and specific targets, sites, areas (Geographical info)
* Provide reports on investigation activities, performance, and successes.
* Conduct and provide Root cause analysis
* Provide and quantify the losses (including consequential losses) – rand value estimates
* Conduct intelligence driven/disruptive operations – minimum 3 per month in WC Province.
* Have a well-established and managed Informer network
* Conduct Covert operations / infiltration by possessing all the necessary resources – people, tools and technology etc.
* Shall arrange and participate in carrying out entrapment (Section 252A)
* Be able to track/trace profile and establish ownership, e.g. suspected vehicles, telephone numbers, etc.
* Service on and as requested by Eskom (Ad-hoc/specific): e.g. deeds, company information, individual information, criminal records, verification of documentation regarding identification/certifications/registrations etc.
* Social media network monitoring for security threats against Eskom network infrastructure i.e. overhead, underground lines, substations and other critical infrastructure in the Grid;
* Transfer of skill, investigation information and workplace experience to Eskom security teams must be conducted by service provider;
* At the end of the contract – Eskom IP to be handed back to Eskom Security Contract Service
* Manager (Corporate memory to be with Eskom Holdings) within 30 calendar days;
* Form Part of disruptive Operations with various law enforcement agencies within the Grid , provide report of outcomes of each operation including any successes;
* Targeted Patrols (in hotspot areas)
* Opening of cases with SAPS, completing of dockets on behalf of Eskom
* Testifying in courts
* Apprehend perpetrators
* Networking with relevant stakeholders including farming forums and other neighbourhood security clusters;
* Technology shall be deployed in identified hotpots areas as tasked by the contract service manager
* The technology must be able to delay, deter and detect and send alerts on real time in order to be able to effect arrests.

**DELIVERABLES**

The service provider shall amongst others, deliver the following:

* Daily incident reports, Weekly reports, Monthly reports, quarterly and annual reports, dockets, sanction reports etc;
* Details of criminal cases opened per month and progress feedback;
* The turnaround time per investigation to be determined by the contract service manager upon discussion with service provider per project;
* Successful arrests of suspects and syndicates;
* Report Outcomes of court cases and/or convictions;
* Report on number of meetings held with relevant stakeholders on behalf of Eskom;
* Proof of skill, information and experience transfer;
* Appearance in courts as per subpoenas;
* Number of case dockets opened compared to the number of incidents opened;
* Targeted patrols per hotspot including weekly patrol plans;
* Response time per incident;
* Detect attempted thefts of overhead and underground cables before they are stolen;
* Early warning of attempted thefts and vandalism of Eskom assets;
* GIS mapping of asset location;
* Number of incidents identified from open idea and the outcome;
* Number of entrapments undertaken per month;
* Maintain Informer database and keep it updated;
* Number of disruptive operations per month
* Protect Eskom assets from vandalism and thefts;
* Reduce vandalism and thefts of Eskom assets;
* Decrease supply interruptions;
* Crime maps (for each Grid)
* Progress reports on all criminal and internal departmental cases;
* Identity and location of syndicate members released from prison;
* Number of illegal exports identified and intercepted;
* Electronic backups of all data gathered on monthly basis;
* Root Cause Analysis Reports;
* Number of identification and impact statements provided to the SAPS including the investigating Officers;
* Unannounced visits made to the Scrap Provincial Disposal contractor and findings (minimum 2 times per month per Grid);
* Ensure that all team members and operators working with and having access to Eskom information, networks, forums and data sign the Non-Disclosure Form for submission to Eskom Security Contract Service Manager prior to  Ensure that a training file of all team members/investigators together with clearance certificate from SAPS is submitted to Eskom Security Contract Service Manager prior to start of the contract.

C**ONTRACTOR PERFORMANCE**

The service provider shall issue daily incidents reports, Weekly consolidated reports, Monthly consolidated reports, quarterly and annual reports showing the following:

* Number of incidents investigated including case numbers;
* Number of arrests vs the incidents investigated;
* Reduction of crime against Eskom assets- reduction rate is set at 80% within first 3 months of start.
* Conviction rate – conviction rate is set at 80%;
* 30 minutes response time (air capability)
* 45 minutes reaction time (land)

**NON-PERFORMANCE AND PENALTIES**

Failure to respond within the stipulated time will have a penalty of 30% deducted from monthly total invoice excl vat against the supplier. The response time must be in the service provider’s Prevention Scope and Plan;

* Failure to reduce the crime rate against Eskom assets within stipulated time period will have a penalty of 30% deducted from monthly total invoice excluding vat against the supplier for non performance;
* Failure to submit required reports within stipulated duration will have a penalty of 30% deducted from monthly total invoice excluding vat against the supplier.