Technical white paper

SMMS Foundation Stage Security Risk Assessment

Consultation on a draft licence condition relating to security risk assessments and audits prior to DCC service provision

Table of contents

Introduction

This white paper outlines the approach and the impact of the consultation paper issued on 31st May 2012 by the Department of Energy and Climate Change [a] upon the HP Smart Meter Managed Service (SMMS). The purpose of the consultation is to request views on a draft licence condition relating to security risk assessments and audits in the period before the Data and Communications Company (DCC) provides services to smart meters. This paper asserts that the licence condition will pass Parliamentary scrutiny by the end of 2012 and that the Government will introduce the new security requirement for smart meter provision.

The following requirements are addressed within the consultation:

- Suppliers will be responsible for the end-to-end security of their smart metering system. This includes the smart metering equipment located within a consumer's premises, the communication network between the consumer's premises and the energy supplier, and the energy supplier's head end system, and all business procedures associated with the installation, operation and support of the system.
- As well as security being considered during the technical design phase the implemented security solutions must be proportionate and effective across the full end-to-end system, including relevant business processes.
- Suppliers must implement security assurance regimes in their procurement, contract, and internal management processes.
- The smart metering system must address the security threats to data privacy and confidentiality and from unauthorised access to smart meter functions.
- The supplier has an overarching duty to ensure a secure system is to an "Appropriate Standard". The supplier must conduct a risk assessment; design a solution for their end-to-end system to the desired level; conduct ongoing risk assessments and implement mitigating measures.
- Suppliers must additionally have a security risk audit conducted by suitably qualified, external specialists. The audit must verify that the risk assessment and solution design is in line with industry good practise and appropriate for the services provided; that the risk assessments have been properly determined; and that the mitigating measures are appropriate to treat the identified risks to the desired level.

The SMMS solution is a 'centre of trust' within the end-to-end architecture and has a pivotal role in administering the end-to-end security framework. The solution must have a high level of trust. This includes establishing trusted relationships with devices (e.g., Communications Hubs and Meters), other entities (e.g., Service Users and HP administration staff) and ultimately to establish and maintain consumer confidence in the system.

When is the system secure?

The smart meter system is defined as secure when it is operated to the Appropriate Standard. This standard is defined as a high level of security that is in accordance with industry good practise and is capable of being verified by a Competent Independent Organisation. To meet the standard the supplier must provision the following:-

- Risk Assessment:
    - Initial comprehensive assessment; the first risk assessment must be within 6 months of the licence condition being introduced
    - ongoing risk assessments; annually
    - Proportionate mitigation of the identified risks.
- An Information Security Management System (ISMS) that aligns the security operations with ISO27001:2005 and any subsequent equivalent standard of the ISO that updates replaces or supersedes ISO27001.

- Demonstrate that the supplier is taking the steps necessary to certify the resilience, reliability and security of the end-to-end system to ISO27001.
- The supplier must provision the following:
    - A security policy, to govern the approach to risk assessment and treatment
    - Incident management procedures, to identify and respond to security incidents
    - Business continuity and disaster recovery procedures
    - Access to appropriately qualified security staff
    - Physical security controls to protect equipment that interacts with the smart metering system.
- A Competent Independent Organisation (CIO) must undertake a security audit of the end-to-end system to assess whether the supplier's ISMS provides a level of protection in line with good industry practice that is commensurate with the security risks and that this Information Security Policy is being carried out.
- Senior management within the supplier must demonstrate how they have responded to each independent audit report.

Direction by Government

Potentially there are unknown compliance costs introduced by the role of the Government and the Authority vested within the Energy Act to exercise power of intervention. The supply must respond to directions issued by the Secretary of State and the Authority that relate to establishing and maintaining a secure end-to-end system within the timeframe established by the direction. The response must establish the steps to be taken or will be taken to comply with the direction and documentary evidence to demonstrate compliance. For the purposes of this White Paper no assertions have been made as to these potential directions.

Who is responsible for what?

The scope of the end-to-end systems includes:-

- the smart metering equipment located within a consumer's premises,
- the communication network between the consumer's premises and the energy supplier,
- the energy supplier's head end system,
- all business procedures associated with the installation, operation and support of the system.

A Responsible/Accountable/Consulted/Informed (RACI) matrix is a method for establishing the role for each stakeholder and participant whenever multiple parties are involved:

- R(esponsible) – Who is responsible for actually doing it? This position is responsible that work is done (they are "doers").
- A(ccountable) – Who has authority to approve or disapprove it? This position has responsibility and authority to approve/disapprove the task or action.
- C(onsulted) – Who needs input about the task? Which entities will need to be consulted about the task or action and who will need to provide an input? They are "kept in the loop" by two-way communication.
- I(nformed) – Who needs to be kept informed about the task? Which entities will need to be informed about the task or action? They are "kept in the picture" by one-way communication.

The following high level RACI illustrates who has security implementation responsibility for major deliverables within the end-to-end system:-

RACI matrix for Smart Meter End-to-End system security

End-to-End functions	Energy Supplier	SMSO	Mobile network supplier (Vodafone)	Public Key Supplier (Symantec)	Field installation Contractor	Meter Supplier
Summary function	**Entity**					
Smart Meter Selection	A/R	I				C
Smart Meter Deployment	A	I	I		R	
Meter Configuration information	A	C			I	R
ZigBee security and meter PKI	A	I				R
Smart Meter Firmware (Creation & Deployment)	C	R				A/R
Head End System	C	A/R	I	I		
Communications network for Smart Meter data	R	C	A/R		I	C
Public Key Infrastructure (Head End/Comms Hub)	C	A		R		
Operation of SMMS	C	A/R	C	C		
Backend accounting and call desk system	A/R	C			I	
Incident management procedures, to identify and respond to security incidents	A/R	R	R	R	R	
Business continuity and disaster recovery procedures	A/R	R	R	R		
Access to and use appropriately qualified security staff	A/R	R	R	R		
Physical security controls to protect equipment that interacts with the smart metering system	A/R	R	R	R	R	R
ISO27001	**Entity**					
ISO27001 ISMS required where Entity has a Responsibility within the End-to-End system: a security policy to govern the approach to risk assessment and treatment	R	R	R	R	R	R

This analysis requires all entities providing services within the end-to-end system to show how they align with ISO27001 during the second quarter of 2013.

How does the SMSO meet the Appropriate Standard?

An overview of the Smart Meter Service Operator (SMSO) End-to-end Security Architecture, risk assessment and mitigations must be provided to Energy Suppliers during joint security and architecture workshops. The architecture and security activities may subsequently be modified as part of the due diligence review of activities because interoperability requirements with SMSOs and the Energy Supplier are typically different. This section considers the approach embedded within HP SMMS for due consideration of the required Security Framework.

The consultation paper from DECC introduces security activities that were considered not essential to the Foundation service: focused end-to-end smart meter system risk assessments, ISMS production and independent audits of the total end-to-end system. An Energy Supplier specific security management plan for the end-to-end system will be necessary. This plan needs to ensure compliance with the standards, policies and applicable regulations to be introduced by the Authority.

This paper provides information on the overall security policies, standards, procedures and best practices for the applications/services implemented and maintained by HP Enterprise Services. All deviations, gaps or risks identified during the proposed security assessment (in 2013), will be documented in an Account Security Plan in order for further actions and risk mitigation to be undertaken.

The SMSO's contribution to meeting the Appropriate Standard using HP's SMMS includes the following:-

Requirement 1: An initial comprehensive and then ongoing risk assessments

Security in HP SMMS is based on the ISO 27001 framework. Security capabilities have been developed and are deployed as an integral part of this Service. HP advocates, adopts and uses a risk assessment process that forms the central concept upon which the SMMS security plan is based. Risk assessment is the process of identifying threats to an asset and specifying adequate controls necessary to secure that asset, based on its value to the SMSO and its customers, coupled with the impact of its loss.

Suppliers as the data owner need to take responsibility for identifying the appropriate set of business control objectives required for safeguarding the information assets of the end-to-end system.

Proposal: it is proposed that the SMSO undertakes the initial and subsequent risk assessments of the end-to-end system. This will need cooperation and commitment from the identified RACI contributors to the system as a whole. The method proposed will use the capabilities required of a Competent Independent Organisation. Thus members of the CESG Listed Adviser Scheme (CLAS) and CESG IT Health Check Service Scheme (CHECK) would be used. The Authority mandates the use of this type of qualified resource and capability to achieve the "Appropriate Standard".

Designed to satisfy the requirements of ISO 27001, a systematic examination of the information security threats and vulnerabilities applicable to information assets requires undertaking. The process has been designed to establish the likelihood of such threats occurring, the cost/impact of the threat to the business and the identification of the safeguards or countermeasures designed to reduce the threats to an acceptable level. It also takes into consideration the recommendations within ISO/IEC 27005:2008; the international standard for Information Security Risk Management.

The risk assessment is designed to:

- Identify the information security risks to the assets in scope – hardware, software and/or processes
- Determine the loss to the business if such risks materialize
- Establish the criteria for evaluating risks
- Identify the control processes and countermeasures that will be implemented to protect the assets and manage the risks
- Establish and complete the Risk Register.

This information can be identified through a risk assessment workshop with the key process and asset stakeholders.

In order to facilitate the successful completion of the workshop, the in-scope assets and/or business processes to be reviewed during the workshop need to be identified in advance in

preparation for discussion at the workshop and each attendee should consider the relevant security threats.

The SMSO can then:

- Identify the security risk exposure, as part of the formal risk assessment;
- Derive the security requirements by conducting a gap analysis that will use the requirements and risk appetite required for the Foundation service;
- Define the necessary security controls, processes and procedures within the ISMS for each RACI contributor;
- Define and document the security metrics and records required to effectively manage the end-to-end business and prove compliance;
- Produce and maintain the necessary security documentation to demonstrate compliance including: the Security Policy, Statement of Applicability and necessary procedural documentation;

The SMSO will require specialist security consultants (e.g. CISSP, CISM, CISA, CLAS etc); certified professionals who will be the main point of contact during the process and, as necessary, assign a number of additional similarly qualified consultants at various points to ensure successful audit and then certification in the longer term. Senior management should be involved in the management of the ISMS and form part of the key stakeholders responsible for the implementation of the ISMS and that it is maintained thereby minimizing the risks to the Energy Supplier, other stakeholder organisations and HP operations.

Requirement 2: Proportionate mitigation of the identified risks.

The SMSO can implement and operate an information security management system (ISMS) that covers all elements of HPs delivery to Foundation customers. A clear picture of the security policy, standards and procedures ensure that the business risks are managed proportionately and cost effectively in line with the business needs.

In a world in which Suppliers and customers, along with government and industry, are immutably connected, every link in the supply chain is capable of introducing risk that affects other components. ISO 27001 has real business benefits and should be used to demonstrate commitment to complying with the industry standard for security management. It is a unifying force that lets large organizations standardize on the way they manage security and apply a single process that is easier to maintain and reacts more quickly to change.

The Information Security Risk Assessment must go through the following main steps:

1. Identify assets & asset owners
2. Group the assets
3. Identify potential threats and vulnerabilities
4. Evaluate the initial likelihood of threats
5. Evaluate the business impact
6. Identify existing countermeasures and controls
7. Evaluate the new threat exposure/likelihood
8. Calculate the new risk level and confirm acceptable level of risk
9. Setup the risk treatment
10. Approval of residual risk
11. Follow-up on risk treatment plan

Requirement 3: An Information Security Management System (ISMS)

The SMSO establishes, implements, operates, monitors, reviews, maintains and improves the documented ISMS for its data centres and services within the context of its overall business activities and the risks it faces, as part of the wider organisation.

The proposed structure of an ISMS is illustrated the HP SMMS structure:-

Requirement 4: Demonstrate approach to ISO27001 certification

The services being provided by an SMSO must be supported by ISO27001 and ISAE certifications. Consideration must be given to the steps necessary to certify the resilience, reliability and security of components for which it is responsible.

Proof of certification should include:

- sustained ISO27001 certification for the data centres. Alignment with existing ISO/EIC 27000 series of standards and future DCC security requirements;
- successful demonstration of compliance to ISO auditors and utilisation of this experience to the joint ISMS development for the end to end SMSO service and longer term certification process.

Requirement 5: The supplier must provision a security policy, to govern the approach to risk assessment and treatment

An Information Security Policy has the objective to provide management direction and support for information security in accordance with business requirements, relevant laws and regulations. SMSO security policies and standards apply to the SMMS systems. These policies should be aligned with ISO 270001. The SMSO Security Policies that are relevant to Foundation Service should be accessible and available within a central repository.
In order to provide a shared service and minimize cost, it should be a goal to minimize Supplier specific polices and their corresponding checks and standardize them as much as possible.

Proposal: It is proposed that the SMSO undertakes a check of the service security policy against the applicable parts of the security policy of an Energy Supplier to establish where and if there are any gaps. This would be undertaken by the same resources used to undertake the initial risk assessment.

Requirement 6: The supplier must provision Incident management procedures, to identify and respond to security incidents

The SMSO service includes provision for Incident management as part of the support and maintenance activities. For major Incidents, such as an outage or reduced service delivery, a "major incident" process will ensure timely escalation to senior management within the SMSO and Energy Supplier. At the same time, the investigation and diagnosis is accelerated and coordinated by the nominated "major incident" leadership team. A "major incident" process will complement the Energy Supplier escalation processes by running in parallel, thus ensuring a mechanism for accurate information exchange between the processes, and assuring the Energy Supplier that SMSO's leadership team is pro-actively engaged to resolve major incidents.

Security Monitoring has the objective to detect unauthorized information processing activities. SMSO systems should be monitored to detect deviation from access control policy and record detectable events to provide evidence in case of security incidents. System monitoring allows the effectiveness of controls adopted to be checked and conformity to an access policy model to be verified.

Audit logs recording privileged user access activities, authorized and unauthorized access attempts, system exceptions, and information security events are retained. Audit logs are reviewed and intrusion detection tools implemented to help facilitate timely detection and response to incidents. Physical and logical user access to audit logs is restricted to authorized personnel.

Audit Logs should be sent to a Security and Information Event Management system for management. The logs collected, where technically possible, should include but e not be limited to the following information:

- User IDs;
- Dates and times for log-on and log-off;
- Terminal identity or location if possible;
- Records of successful and rejected system access attempts;
- Records of successful and rejected data and other resource access attempts.

Log information should include user, administrator and operator activities. Logs must be protected and only accessible by those with a need to know.

Monitoring of security events is undertaken in by a security operations centre utilising appropriate Security tools.

Requirement 7: The supplier must provision Business continuity and disaster recovery procedures

Business continuity and disaster recovery services are integral elements of SMSO services. The Service Level Agreement with the Energy Supplier should define the business continuity and disaster recovery needed.

Requirement 8: The supplier must provision Access to and use appropriately qualified security staff

The SMSO should provide a pool of security resources that has the appropriate breadth and depth of security skills. Security management resources within the SMSO should include Chief Security Officer, Account Security Officer, PKI and security subject matter experts. In addition consideration should be given to CESG-approved CLAS consultants who are available to support specific requirements projects and a forensic team and penetration testing team approved under the CESG CHECK scheme.

Requirement 9: The supplier must provision Physical security controls to protect equipment that interacts with the smart metering system.

Security controls for data centres should be audited to ISAE3402. These controls are in line with those required for HMG approved data centres and both are already supporting Government project work. The following summary is an overview of the physical measures, service continuity management and internal countermeasures that can be used to protect smart meter data within data centres.

Physical overview

Multi layered security mitigates and protects against any individual component failure:

- Physical Security is multi layered and starts at the site boundary and continues all the way through to the IT equipment cabinets.
- All staffs are security cleared.
- Access to IT equipment is controlled by a Permit to Work system.
- Security procedures include mandatory pre-notification of all visitors and all deliveries.
- Site Threat Levels determined by intelligence from Local and National Police, CPNI, and HP Security.
- Site Response Levels are determined by the threat level and type of threat.

IT Service continuity

- Paired data centres via private dark fibre circuits.
- No shared risks or infrastructure services are common to both sites.
- Full threat assessments are carried out for both sites and reviewed annually.
- Neither site is in a flood plain or under flight paths.
- The sites are fed from different primary substations off the National Grid.
- Both sites fed from different and diverse digital exchanges from multiple telecomm carriers.
- No military or hazardous installations are close to either site.

Internal countermeasures

- "Fail Secure" locks are used.
- Access Card and Biometric readers
- Highest security rating on locks and doors to the data halls and communications rooms.
- Anti-tailgating portal doors are deployed.
- Unique keys are used for IT cabinets.
- The Electronic Key Management System releases cabinet keys only to authorised staff.
- Doors are monitored for door and bolt position, and status.
- Electronic Beam motion detection and CCTV is used throughout.
- High Security wall construction is used.
- Ram and climb resistant perimeter fencing includes intrusion detection.
- Protection against power loss, fire and flood.
- Temperature controlled and protected against humidity.

How will the end-to-end system be audited?

The ISMS representing the end-to-end system must be audited by a CIO with competence that is documented. The task of providing a risk assessment with qualified resource and undertake regular audits will need to be included within the planning for the end-to-end system.

It is proposed that a Security Working Group (SWG) is formed by the stakeholder organisations to establish governance for this process and establish the Appropriate Standard for each of the RACI service providers.

Initial estimated business costs for each party can then be collected and relevant investment plans and delivery expectations can be set. Part of this data collection activity will be establishing what is required from the CIO, whether a Request for Quotation is issued, identification of at least two potential Suppliers and how it will be funded.

Requirement 10: Engage a Competent Independent Organisation

The CIO must undertake a security audit of the end-to-end systems to assess whether the supplier's ISMS provides a level of protection in line with good industry practice that is commensurate with the security risks. This must be done no later than six months after the licence condition comes into force and at least once in each subsequent year.

The SWG should undertake the identification and recommendation of the CIO and jointly (and internally within each stakeholder organisation), obtain business approvals to proceed. This group needs to be formed within the next 6 months to be able to respond to the Authority planning to issue a new licence condition by the end of 2012.

The SWG should also issue a joint plan for audit for the service to meet the Authority expectations. Implementation and compliance risks will need to be captured within the Risk Register for the programme.

Many existing applications were not designed to run in a potentially hostile environment (there is an expectation that the threat level is significant within the end-to-end system), thus there is a need to build in security at the application and data level. The Head End system application should be reviewed, inspected and tested before deploying; this exercise should be guided by the output of the risk-based assessment. For example, undertaking Application penetration testing of the HES and Infrastructure penetration testing as part of the service.

Requirement 11: Senior management responsibility

Senior management within the SMSO and sub-contractors must demonstrate how they have responded to each independent audit report. Accountability will be with each Energy Supplier however the SWG should provide the governance mechanism for establishing the "what, when and how", for the mitigations or corrective actions that may need to be undertaken.

Recommendations include the following broad steps as part of a security program:

1. Establish the risk-based approach as discussed within this paper.

2. Design applications to securely run.

3. Implement ongoing auditing and management.

4. Assess infrastructure (and platform) security during service running.

An overall view of the security operations, risk, compliance, is recommended. A comprehensive integrated view of the security posture, risk level, and compliance status should be available to senior management.

Continuous monitoring and maintenance of security incident records and log files are crucial to enabling forensic examination and analysis in the event that a security breach or disclosure occurs. This information should be available in real time to facilitate rapid response, notification, and containment measures. A single, graphical, executive-level dashboard of enterprise security status that aligns information security at a corporate level is a useful mechanism, including the provision of real-time views of current security events that in turn improves control of security projects, audits, budgets, and performance. Reporting actual metrics and return on investment (ROI) enables the communication of the value of security implemented within the end-to-end system and addresses risk.

Call to action

It is proposed that the following actions are undertaken over the next period of 6 months:-

- SMSOs should consider an initial risk assessment of the end-to-end system. This will need cooperation and commitment from the identified RACI contributors to the systems as a whole. The method proposed will use the capabilities required of a Competent Independent Organisation (e.g., CLAS and CHECK). It is unclear at present how the Authority or stakeholders will fund this initial work.
- That a Security Working Group (SWG) is formed by the stakeholder organisations to establish governance for this process and establish the Appropriate Standard for each of the RACI service providers.
- That the SWG determine the initial ISO27001 Gap Analysis between existing ISO certifications and Authority defined end-to-end "Appropriate Standard" for each stakeholder organisation. This will ensure compliance with the Authorities specific standards, policies and applicable regulations especially where it relates to "Change of Supplier".
- Each stakeholder organisation reports to the SWG an estimate of the business cost, investment and deployment plan to close the identified Gaps. The SWG should then create and publish a plan for implementation and ISO27001 certification for the end-to-end system.
- Each stakeholder organisation should then obtain business approvals to proceed and execute the business plan over an 18 month window.

Referenced documentation

The following table lists the documentation which are referenced in this white paper

Reference	Document Name	Short Description of Referenced Document
a	"Smart Metering Implementation Programme Consultation on a draft licence condition relating to security risk assessments and audits in the period before the DCC provides services to smart meters" 31 May 2012. Department of Energy and Climate Change	Proposed new license condition for security assurance of smart meter systems

Document Information

Project Name:	Smart Meter Managed Service		
Prepared By:	Andy Burgess	Document Version No:	1.0
Title:	SMMS Foundation Stage Security Risk Assessment	Document Version Date:	25 July 2012
Document Owner:	HP Enterprise Security Services (ESS)	Review Date*:	
Reviewed By:			

*Review Date must be at least a year from the document version date.

Distribution List

From	Date	Phone/Fax/Email

To	Action*	Due Date	Phone/Fax/Email
	Approve		
	Approve		
	Approve		

* Action Types: Approve, Review, Inform, File, Action Required, Attend Meeting, Other (please specify)

Table 1: Version History	Ver. Date	Revised By	Description	Reviewer	Status
0.1	8 June 2012	Andy Burgess	Initial Draft		Draft
0.2	11 June 2012	Andy Burgess	Incorporated review comments	Andrew Shephard	Draft
0.3	15 June 2012	Andy Burgess	Incorporated review comments and referenced SMMS users as Energy Suppliers	Andy Broekhuizen	Draft
0.4	23 July 2012	Andy Burgess	Further minor amendments	Andy Burgess	Draft
1.0	25 July 2012	Andy Burgess	Updated to version 1	Andy Burgess	Issued

Glossary

The table below contains definitions of the terms used in this document:

Term	Definition
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Incident	A system/device, network, application or associated data that is maintained by or on behalf of HP is compromised or under attack. For example, web server defacements, denial-of-service attacks, account break-ins and hostile/ unapproved vulnerability scanning and cracking activities.
Risk	A combination of: (i) the likelihood that a particular vulnerability in an information system will be either intentionally or unintentionally exploited by a particular threat resulting in a loss of confidentiality, integrity, or availability, and (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability will have on HP operations (including mission, functions, image or reputation), HP assets, or individuals (including privacy) should the exploitation occur.
Risk Assessment	A key component of risk management that brings together important information with regard to the protection of information and information systems including the identification of: (i) threats and vulnerabilities, and (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on HP and SMMS Customer operations (including mission, functions, image or reputation), HP and SMMS Customer assets (Considered in the SMMS Customer context), or individuals (including privacy) should there be a threat exploitation of information system vulnerabilities.
Risk Management	The process of identifying, controlling, and mitigating risks. It includes risk assessment, cost benefit analysis, and the selection, implementation, testing and evaluation of security controls.
Security Assessment	An assessment is the measurement, by a third party, of a service against security industry best practices. See RISK ASSESSMENT, SECURITY AUDIT and SECURITY REVIEW.
Security Audit	An audit is the measurement, by a third party or customer representative, of a service against established policy. See SECURITY ASSESSMENT and SECURITY REVIEW.
Security Controls	The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.
Security Review	A review is the measurement, self-performed, of a service against established policy and industry best practices. See SECURITY ASSESSMENT and SECURITY AUDIT.
Third Party	Individuals or organizations who are not HP or customer Employees and not under direct HP management or customer Management.
Threat	Any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability.
Vulnerability	A flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect HP or SMMS operations (including mission, functions, image or reputation), HP or SMMS assets, or individuals (including privacy) through a loss of confidentiality, integrity, or availability.

Get connected

hp.com/go/getconnected

Current HP driver, support, and security alerts
delivered directly to your desktop

4AA4-5MMSENN, Created July 2012