

# What's New

GSA Expands MAS Solutions to Maximize Data Protection and Minimize Agencies' Risk



## New Service Offerings and a BPA Meet Demands for Data and Information Security

When it comes to adaptability for your data-protection needs, you can count on GSA to listen to and work with you – and also to meet your requirements. We can help you reflect on past functionality and identify areas needing improvement, and we provide you with solutions for a secure, successful tomorrow. That is why so many federal agencies rely on GSA to provide reactive (in addition to proactive) solutions, like the five new Special Item Numbers (SINs) and the Blanket Purchase Agreement (BPA) available through GSA's Financial and Business Services (FABS) Multiple Award Schedule (MAS) 520.

Whenever you choose from our full breadth of information-protection services, you will receive the new, specialized service offerings now available under the five new SINs (Special Item Numbers) of our FABS MAS. The services available under these SINs encompass the full range of solutions that your agency needs to protect against and respond to a breach of Personally Identifiable Information (PII), Personal Health Information (PHI), and other sensitive data. Included are proactive ("pre-breach") services, such as risk-assessment and mitigation services, as well as reactive ("post-breach") services, which include independent risk analysis, credit monitoring, and data-breach analysis.

These new SINs complement a credit-monitoring BPA also in place under the FABS MAS. This BPA provides an impressive selection of specialized solutions to meet your agency's existing and emerging protection needs. (Please note that a BPA is an agreement – established under a GSA MAS – that allows vendors to provide supplies and services at a low-dollar value and at high volume for a specified term or period of time, normally not to exceed five years.)

Taking acquisition simplicity to an even higher level for services covered by these five new SINs, GSA also enables you to establish

your own smart BPAs that are continuous, repeat or ongoing.

This means you can create your own BPAs – with any number of contractors – for the wide array of services offered via these new SINs, that cover the gamut of the identity-protection industry. Establishing BPAs for these services – which you are encouraged to do – allows you to realize cost- and efficiency-savings offered through such an arrangement. Plus, it simplifies your recurring orders for services, for both your agency and the BPA vendor, by reducing administrative time and paperwork.

The comprehensive services covered by these new SINs are crucial solutions that protect against threats – especially for data protection and privacy – needed in today's world. They are:

- **Risk-assessment and mitigation services;**
- **Independent risk analysis;**
- **Data-breach analysis;**
- **Comprehensive protection solutions; and**
- **Program-management services.**

As a service agency that's 100-percent customer-focused, GSA exists to meet your acquisition needs and fulfill the evolving requirements of all federal agencies. To assist you, we offer knowledgeable, competent procurement professionals that you can turn to – and always count on – for any of the millions of products, services and solutions we offer. We are ready to serve you, while ensuring that you receive the best value in selection, price, availability, service, quantity and quality. Our focus on strategic sourcing includes accommodating your every need with streamlined processes, including simplified and efficient ordering and order fulfillment.

**One Country. One Mission. One Source.**



If you need pre- or post-breach assistance – a total solution or a more targeted one – GSA has the answer. Refer to the SIN descriptions below to find your solutions.

### 520-17 – Risk Assessment and Mitigation Services (NAICS 541990)

The Risk Assessment and Mitigation Services SIN includes, but is not limited to, the following:

- Documentation of disclosure responsibilities for Personally Identifiable Information (PII) and Personal Health Information (PHI);
- Deployment of risk-assessment and mitigation strategies and techniques;
- Improvement of capabilities through the reduction, identification and mitigation of risks;
- Detailed risk statements, risk explanations, and mitigation recommendations;
- Design and development of new business applications, processes and procedures in response to risk assessments;
- Ensuring compliance with government and regulatory requirements;
- Evaluation of threats and vulnerabilities to the protection of PII- and PHI-type data;
- Training of government personnel on how to prevent data breaches and identity theft;
- Information assurance of PII- and PHI-type information;
- Vulnerability assessments;
- Privacy impact and policy assessments;
- Review and creation of privacy and safeguarding policies;
- Prioritization of threats;
- Maintenance and demonstration of compliance; and
- Evaluation and analysis of internal controls critical to the detection and elimination of weaknesses to the protection of PII- and PHI-type data.

### 520-18 – Independent Risk Analysis (NAICS 561611)

The Independent Risk Analysis SIN includes a review of all information compromised by a data breach for trends and unusual patterns. The circumstances surrounding the breach are investigated to determine whether it appears to be incidental, accidental or targeted. The breached data itself is analyzed to determine if there is any current evidence of organized misuse. Ultimately, the analysis provides a determination concerning the probability that breached data may be used to harm the individual(s) whose personal information has been compromised. The tasks involved in

independent risk analysis include, but are not limited to, the following:

- Monitoring of multiple data elements and sources;
- Metadata analysis;
- Pattern analysis;
- Risk analysis;
- Privacy impact analysis;
- Statistical analysis;
- Data-structure development;
- Notification services;
- Probability analysis to determine if breached data has been used to cause harm;
- Determination of the level of risk for potential misuse of sensitive PII- and PHI-type data;
- Certification of findings regarding the misuse of compromised data;
- Investigation of circumstances surrounding breach, including digital forensic analysis;
- Collection of evidence regarding data breaches; and
- Development of a risk-mitigation plan.

### 520-19 – Data Breach Analysis (NAICS 561611)

The Data Breach Analysis SIN includes the monitoring and detection of breached identities and PII- and PHI-type data across multiple industries, in order to detect patterns of misuse related to a specific data loss. The breached files are continuously monitored for a period of weeks, months or years. Also, the services under this SIN can provide the locations of potential misuse for further law enforcement action, as well as a list of consumers likely to be fraud victims. The tasks involved include, but are not limited to, the following:

- Monitoring of multiple non-credit data elements and sources;
- Fraud detection and protection solutions;
- Fraud resolution and assistance for affected individuals;
- Fraud alerts;
- Corrective actions;
- Notification services;
- Identity-theft insurance (as allowed by applicable state statutes);
- Social Security-number monitoring; and
- Credit-card monitoring.

### 520-20 – Comprehensive Protection Solutions (NAICS 541990)

The Comprehensive Protection Solutions SIN allows for customized solutions that integrate the services found under SIN 520-16 Business Information

Services (Credit Monitoring Services), 520-17 Risk Assessment and Mitigation Services, 520-18 Independent Risk Analysis and 520-19 Data Breach Analysis. This SIN cannot be used to fulfill requirements that fall within the scope of one of the other four SINs. It may only be used to fulfill agency requirements that span across multiple SINs.

### 520-21 – Program Management Services (NAICS 541611)

The Program Management Services SIN encompasses the management of financial and business solutions programs and projects and includes, but is not limited to: program management, program oversight, project management, and program integration of a limited duration. A variety of functions may be utilized to support program integration or project-management tasks.

Note: Services not authorized for purchase under this SIN are services whose primary purpose or the preponderance of work performed is specifically covered by another GSA MAS, such as: mission-oriented business services covered by GSA MAS 874; engineering services covered by GSA MAS 871; IT services covered by GSA MAS 70; advertising and marketing services covered by GSA MAS 541; human resources services covered by GSA MAS 738 X; logistics services covered by GSA MAS 874 V; security services covered by GSA MAS 84; transportation services covered by GSA MAS 48; travel services covered by GSA MAS 599; environmental services covered by GSA MAS 899; language services covered by GSA MAS 738 II; and training services covered by GSA MAS 69.

### 520-16 – Business Information Services

Credit-monitoring services have been offered under this category for some time. In August 2006, GSA established BPAs with three contractors for credit-monitoring services that include:

- Social Security-number monitoring;
- One- or three-bureau credit-report monitoring;
- Credit-card registry;
- Identity-theft insurance; and
- Assistance with fraud resolution.

For more information, visit the GSA Schedules eLibrary overview at [www.gsa.gov/elibrary](http://www.gsa.gov/elibrary), where you can access the GSA Schedule eLibrary Web site to learn about GSA MAS 520 or other GSA Schedules. If you want further information about the other services listed here, please contact Stephanie Cooke via e-mail at [stephanie.cooke@gsa.gov](mailto:stephanie.cooke@gsa.gov) or phone at (703) 605-2858, or Shontae Harley via e-mail at [shontae.harley@gsa.gov](mailto:shontae.harley@gsa.gov) or phone at (703) 605-2816.